ESET MAIL SECURITY

PARA MICROSOFT EXCHANGE SERVER

Manual de instalación y Guía del usuario

Microsoft® Windows® Server 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Haga clic aquí para descargar la versión más reciente de este documento

ENJOY SAFER TECHNOLOGY™

ESET **MAIL SECURITY**

Copyright ©2016 **de ESET, spol. s r.o.**
ESET Mail Security ha sido desarrollado por ESET, spol. s r.o.

Para obtener más información, visite el sitio www.eset.com.
Todos los derechos reservados. Ninguna parte de esta documentación podrá reproducirse, almacenarse en un sistema de recuperación o transmitirse en forma o modo alguno, ya sea por medios electrónicos, mecánicos, fotocopia, grabación, escaneo o cualquier otro medio sin la previa autorización por escrito del autor.
ESET, spol. s r.o. se reserva el derecho de modificar cualquier elemento del software de la aplicación sin previo aviso.

Servicio de atención al cliente: www.eset.com/support

REV. 19/05/2016

Contenido

1. Introducción....6
1.1 Novedades de la versión 6....6
1.2 Páginas de Ayuda....7
1.3 Métodos utilizados....7
1.3.1 Protección de la base de datos de buzones....8
1.3.2 Protección del correo electrónico....8
1.3.3 Análisis de la base de datos a petición....8
1.4 Tipos de protección....10
1.4.1 Protección antivirus....10
1.4.2 Protección Antispam....10
1.4.3 Aplicación de reglas definidas por el usuario....11
1.5 Interfaz de usuario....11
1.6 Administración a través de ESET Remote Administrator....12
1.6.1 ERA Server....12
1.6.2 Web Console....13
1.6.3 Agente....14
1.6.4 Sensor RD....14
1.6.5 Proxy....14
2. Requisitos del sistema....15
3. Instalación....16
3.1 Pasos de instalación de ESET Mail Security....17
3.1.1 Instalación de la línea de comandos....20
3.2 Activación del producto....23
3.3 Terminal Server....23
3.4 ESET AV Remover....24
3.5 Actualización a una versión más reciente....24
3.6 Roles de Exchange Server: perimetral y concentrador....24
3.7 Roles de Exchange Server 2013....25
3.8 Protección antispam y conector POP3....25
4. Guía para principiantes....27
4.1 Interfaz de usuario....27
4.2 Archivos de registro....29
4.2.1 Registro del análisis....31
4.3 Análisis....33
4.3.1 Análisis Hyper-V....35
4.4 Cuarentena de correo electrónico....36
4.4.1 Detalles del correo electrónico en cuarentena....38
4.5 Actualización....39
4.5.1 Configuración de la actualización de la base de firmas de virus....40
4.5.2 Configuración del servidor proxy para las actualizaciones....40
4.6 Configuración....41
4.6.1 Servidor....41
4.6.2 Ordenador....42
4.6.3 Herramientas....44
4.6.4 Importar y exportar configuración....45
4.7 Herramientas....46
4.7.1 Procesos en ejecución....47
4.7.2 Observar actividad....49
4.7.2.1 Selección del período de tiempo....50
4.7.3 ESET Log Collector....50
4.7.4 Estadísticas de protección....51
4.7.5 Clúster....52
4.7.6 ESET Shell....54
4.7.6.1 Uso....55
4.7.6.2 Comandos....59
4.7.6.3 Archivos por lotes/Creación de scripts....61
4.7.7 ESET SysInspector....62
4.7.7.1 Crear un informe del estado del sistema....62
4.7.7.2 ESET SysInspector....62
4.7.7.2.1 Introducción a ESET SysInspector....62
4.7.7.2.1.1 Inicio de ESET SysInspector....63
4.7.7.2.2 Interfaz de usuario y uso de la aplicación....63
4.7.7.2.2.1 Controles de programa....63
4.7.7.2.2.2 Navegación por ESET SysInspector....65
4.7.7.2.2.1 Accesos directos del teclado....66
4.7.7.2.2.3 Comparar....67
4.7.7.2.3 Parámetros de la línea de comandos....68
4.7.7.2.4 Script de servicio....69
4.7.7.2.4.1 Generación de scripts de servicio....69
4.7.7.2.4.2 Estructura del script de servicio....69
4.7.7.2.4.3 Ejecución de scripts de servicio....72
4.7.7.2.5 Preguntas frecuentes....72
4.7.7.2.6 ESET SysInspector como parte de ESET Mail Security....74
4.7.8 ESET SysRescue Live....74
4.7.9 Planificador de tareas....74
4.7.10 Enviar muestras para su análisis....78
4.7.10.1 Archivo sospechoso....79
4.7.10.2 Sitio web sospechoso....79
4.7.10.3 Archivo de falso positivo....79
4.7.10.4 Sitio de falso positivo....80
4.7.10.5 Otros....80
4.7.11 Cuarentena....80
4.8 Ayuda y asistencia técnica....81
4.8.1 Cómo....82
4.8.1.1 Cómo actualizar ESET Mail Security....82
4.8.1.2 Cómo activar ESET Mail Security....83
4.8.1.3 Cómo cuenta ESET Mail Security los buzones de correo....83
4.8.1.4 Cómo crear una tarea nueva en Tareas programadas....84
4.8.1.5 Cómo programar una tarea de análisis (cada 24 horas)....85
4.8.1.6 Cómo eliminar un virus del servidor....85
4.8.2 Enviar una solicitud de soporte....85
4.8.3 Limpiador especializado ESET....86
4.8.4 Acerca de ESET Mail Security....86
4.8.5 Activación del producto....86

4.8.5.1 Registro ... 87
4.8.5.2 Activación de Administrador de seguridad ... 87
4.8.5.3 Error de activación ... 87
4.8.5.4 Licencia ... 88
4.8.5.5 Progreso de la activación ... 88
4.8.5.6 La activación se ha realizado correctamente ... 88

5. Trabajo con ESET Mail Security ... 89

5.1 Servidor ... 90
5.1.1 Configuración de prioridad de agentes ... 91
5.1.1.1 Modificar prioridad ... 91
5.1.2 Configuración de la prioridad del agente ... 91
5.1.3 Antivirus y antiespía ... 92
5.1.4 Protección Antispam ... 93
5.1.4.1 Filtrado y verificación ... 94
5.1.4.2 Configuración avanzada ... 95
5.1.4.3 Configuración de lista gris ... 98
5.1.5 Reglas ... 100
5.1.5.1 Lista de reglas ... 100
5.1.5.1.1 Asistente de reglas ... 101
5.1.5.1.1.1 Condición de la regla ... 102
5.1.5.1.1.2 Acción de la regla ... 103
5.1.6 Protección de la base de datos de buzones ... 104
5.1.7 Protección del correo electrónico ... 105
5.1.7.1 Configuración avanzada ... 107
5.1.8 Análisis de la base de datos a petición ... 108
5.1.8.1 Elementos de buzón de correo adicionales ... 110
5.1.8.2 Servidor Proxy ... 110
5.1.8.3 Detalles de la cuenta de análisis de la base de datos ... 110
5.1.9 Cuarentena de correo electrónico ... 112
5.1.9.1 Cuarentena local ... 112
5.1.9.1.1 Almacenamiento de archivos ... 113
5.1.9.1.2 Interfaz web ... 115
5.1.9.2 Buzón en cuarentena y cuarentena de MS Exchange ... 119
5.1.9.2.1 Configuración del administrador de la cuarentena ... 119
5.1.9.2.2 Servidor proxy ... 120
5.1.9.3 Detalles de la cuenta del administrador de la cuarentena ... 121
5.1.10 Clúster ... 121
5.1.10.1 Asistente de clúster: página 1 ... 123
5.1.10.2 Asistente de clúster: página 2 ... 125
5.1.10.3 Asistente de clúster: página 3 ... 126
5.1.10.4 Asistente de clúster: página 4 ... 128

5.2 Ordenador ... 131
5.2.1 Detección de una amenaza ... 132
5.2.2 Exclusiones de procesos ... 133
5.2.3 Exclusiones automáticas ... 134
5.2.4 Caché local compartida ... 134
5.2.5 Rendimiento ... 135
5.2.6 Protección del sistema de archivos en tiempo real ... 135
5.2.6.1 Exclusiones ... 136
5.2.6.1.1 Agregar o modificar exclusiones ... 137
5.2.6.1.2 Formato de exclusión ... 137
5.2.6.2 Parámetros de ThreatSense ... 137
5.2.6.2.1 Extensiones de archivo excluidas del análisis ... 140
5.2.6.2.2 Parámetros adicionales de ThreatSense ... 141
5.2.6.2.3 Niveles de desinfección ... 141
5.2.6.2.4 Modificación de la configuración de protección en tiempo real ... 142
5.2.6.2.5 Análisis de protección en tiempo real ... 142
5.2.6.2.6 Qué debo hacer si la protección en tiempo real no funciona ... 142
5.2.6.2.7 Envío de archivos ... 142
5.2.6.2.8 Estadísticas ... 143
5.2.6.2.9 Archivos sospechosos ... 143
5.2.7 Análisis del ordenador a petición y análisis Hyper-V ... 144
5.2.7.1 Inicio del análisis personalizado y del análisis Hyper-V ... 144
5.2.7.2 Progreso del análisis ... 147
5.2.7.3 Administrador de perfiles ... 148
5.2.7.4 Objetos de análisis ... 149
5.2.7.5 Interrupción de un análisis programado ... 149
5.2.8 Análisis de estado inactivo ... 149
5.2.9 Análisis en el inicio ... 150
5.2.9.1 Verificación de la ejecución de archivos en el inicio ... 150
5.2.10 Medios extraíbles ... 151
5.2.11 Protección de documentos ... 151
5.2.12 HIPS ... 152
5.2.12.1 Reglas de HIPS ... 153
5.2.12.1.1 Configuración de regla de HIPS ... 153
5.2.12.2 Configuración avanzada ... 155
5.2.12.2.1 Controladores con carga siempre autorizada ... 155

5.3 Actualizar ... 155
5.3.1 Reversión de actualización ... 156
5.3.2 Tipo de actualización ... 157
5.3.3 Servidor Proxy HTTP ... 157
5.3.4 Conectarse a la LAN como ... 158
5.3.5 Mirror ... 159
5.3.5.1 Actualización desde el servidor Mirror ... 161
5.3.5.2 Archivos replicados ... 162
5.3.5.3 Resolución de problemas de actualización del Mirror ... 162
5.3.6 Cómo crear tareas de actualización ... 163

5.4 Web y correo electrónico ... 163
5.4.1 Filtrado de protocolos ... 163
5.4.1.1 Aplicaciones excluidas ... 164
5.4.1.2 Direcciones IP excluidas ... 164
5.4.1.3 Clientes de correo electrónico y web ... 164
5.4.2 SSL/TLS ... 165
5.4.2.1 Comunicación SSL cifrada ... 166
5.4.2.2 Lista de certificados conocidos ... 166
5.4.3 Protección del cliente de correo electrónico ... 167
5.4.3.1 Protocolos de correo electrónico ... 167
5.4.3.2 Alertas y notificaciones ... 168
5.4.3.3 Barra de herramientas de MS Outlook ... 168

Contenido

5.4.3.4 Barra de herramientas de Outlook Express y Windows Mail ... 169
5.4.3.5 Cuadro de diálogo de confirmación ... 169
5.4.3.6 Analizar de nuevo los mensajes ... 169
5.4.4 Protección del tráfico de Internet ... 169
5.4.4.1 Básico ... 170
5.4.4.2 Gestión de direcciones URL ... 170
5.4.4.2.1 Crear nueva lista ... 171
5.4.4.2.2 Direcciones HTTP ... 171
5.4.5 Protección Anti-Phishing ... 172

5.5 Control de dispositivos ... 173
5.5.1 Reglas de control de dispositivos ... 173
5.5.2 Adición de reglas de control de dispositivos ... 174
5.5.3 Dispositivos detectados ... 175
5.5.4 Grupos de dispositivos ... 175

5.6 Herramientas ... 176
5.6.1 ESET Live Grid ... 176
5.6.1.1 Filtro de exclusión ... 177
5.6.2 Cuarentena ... 177
5.6.3 Microsoft Windows Update ... 177
5.6.4 Proveedor WMI ... 178
5.6.4.1 Datos proporcionados ... 178
5.6.4.2 Acceso a datos proporcionados ... 183
5.6.5 Objetos de análisis de ERA ... 183
5.6.6 Archivos de registro ... 183
5.6.6.1 Filtrado de registros ... 184
5.6.6.2 Buscar en el registro ... 185
5.6.6.3 Mantenimiento de registros ... 186
5.6.7 Servidor proxy ... 187
5.6.8 Notificaciones por correo electrónico ... 187
5.6.8.1 Formato de mensajes ... 188
5.6.9 Modo de presentación ... 188
5.6.10 Diagnóstico ... 189
5.6.11 Atención al cliente ... 189
5.6.12 Clúster ... 190

5.7 Interfaz de usuario ... 191
5.7.1 Alertas y notificaciones ... 192
5.7.2 Configuración de acceso ... 193
5.7.2.1 Contraseña ... 193
5.7.2.2 Configuración de la contraseña ... 193
5.7.3 Ayuda ... 193
5.7.4 ESET Shell ... 193
5.7.5 Desactivar la GUI en Terminal Server ... 194
5.7.6 Mensajes y estados desactivados ... 194
5.7.6.1 Mensajes de confirmación ... 194
5.7.6.2 Estados de aplicación desactivados ... 194
5.7.7 Icono en la bandeja del sistema ... 195
5.7.7.1 Pausar la protección ... 195
5.7.8 Menú contextual ... 196

5.8 Restaurar la configuración de esta sección ... 196

5.9 Restaurar la configuración predeterminada ... 197

5.10 Tareas programadas ... 197
5.10.1 Detalles de la tarea ... 198
5.10.2 Repetición de la tarea: Una vez ... 199
5.10.3 Repetición de la tarea ... 199
5.10.4 Repetición de la tarea: Diariamente ... 199
5.10.5 Repetición de la tarea: Semanalmente ... 199
5.10.6 Repetición de la tarea: Desencadenada por un suceso ... 199
5.10.7 Detalles de la tarea: Ejecutar aplicación ... 199
5.10.8 Detalles de la tarea - Enviar informes de cuarentena de correo electrónico ... 200
5.10.9 Tarea omitida ... 200
5.10.10 Detalles de la tarea planificada ... 200
5.10.11 Perfiles de actualización ... 200
5.10.12 Creación de tareas nuevas ... 201

5.11 Cuarentena ... 202
5.11.1 Copiar archivos en cuarentena ... 203
5.11.2 Restauración de archivos de cuarentena ... 203
5.11.3 Envío de un archivo a cuarentena ... 203

5.12 Actualizaciones del sistema operativo ... 204

6. Glosario ... 205

6.1 Tipos de amenazas ... 205
6.1.1 Virus ... 205
6.1.2 Gusanos ... 205
6.1.3 Caballos troyanos ... 206
6.1.4 Rootkits ... 206
6.1.5 Adware ... 206
6.1.6 Spyware ... 207
6.1.7 Empaquetadores ... 207
6.1.8 Bloqueador de exploits ... 207
6.1.9 Análisis avanzado de memoria ... 208
6.1.10 Aplicaciones potencialmente peligrosas ... 208
6.1.11 Aplicaciones potencialmente indeseables ... 208

6.2 Correo electrónico ... 208
6.2.1 Publicidad ... 209
6.2.2 Información falsa ... 209
6.2.3 Phishing ... 209
6.2.4 Reconocimiento de correo no deseado no solicitado ... 210
6.2.4.1 Reglas ... 210
6.2.4.2 Filtro Bayesiano ... 210
6.2.4.3 Lista blanca ... 211
6.2.4.4 Lista negra ... 211
6.2.4.5 Control del servidor ... 211

1. Introducción

ESET Mail Security 6 para Microsoft Exchange Server es una solución integrada que protege los buzones de correo ante diversos tipos de contenido malicioso, como archivos adjuntos infectados por gusanos o troyanos, documentos que contienen scripts dañinos, phishing y spam. ESET Mail Security proporciona tres tipos de protección: antivirus, antispam y reglas definidas por el usuario. ESET Mail Security elimina el contenido malicioso en el servidor de correo, antes de que llegue a la bandeja de entrada del cliente de correo electrónico del destinatario.

ESET Mail Security es compatible con Microsoft Exchange Server versión 2003 y posteriores, así como con Microsoft Exchange Server en un entorno de clúster. En las versiones más recientes (Microsoft Exchange Server 2003 y posteriores), también se admiten roles específicos (buzón de correo, concentrador, perimetral). Puede administrar ESET Mail Security de forma remota en redes más grandes con la ayuda de ESET Remote Administrator.

Además de ofrecer la protección de Microsoft Exchange Server, ESET Mail Security tiene también las herramientas necesarias para garantizar la protección del servidor (protección residente, protección del tráfico de Internet y protección del cliente de correo electrónico).

1.1 Novedades de la versión 6

- Administrador de la cuarentena de correo electrónico: el administrador puede inspeccionar los objetos de esta sección de almacenamiento y optar por eliminarlos o liberarlos. Esta función permite gestionar con sencillez los correos electrónicos que pone en cuarentena el agente de transporte.
- Interfaz web de la cuarentena de correo: se trata de una alternativa web al administrador de la cuarentena de correo electrónico.
- Antispam: este componente esencial se ha sometido a una importante renovación, y ahora utiliza un nuevo y galardonado motor con un rendimiento mejorado.
- Análisis de la base de datos a petición: el módulo de análisis de la base de datos a petición utiliza la API de EWS (Exchange Web Services) para conectarse a Microsoft Exchange Server a través de HTTP/HTTPS. Además, el módulo de análisis ejecuta análisis en paralelo para mejorar el rendimiento.
- Reglas: este menú permite a los administradores definir manualmente las condiciones de filtrado de correo electrónico y las acciones que se deben realizar con los mensajes de correo electrónico filtrados. Las reglas de la versión más reciente de <%PN%> se han rediseñado para permitir más flexibilidad, lo que concede al usuario todavía más posibilidades.
- Clúster de ESET: de una forma parecida a ESET File Security 6 para Microsoft Windows Server, la unión de estaciones de trabajos a nodos ofrecerá automatización de la gestión adicional gracias a la posibilidad de distribuir una política de configuración entre todos los miembros del clúster. La creación de los propios clústeres puede efectuarse con el nodo instalado, el cual puede posteriormente instalar e iniciar todos los nodos de forma remota. Los productos para servidor de ESET se pueden comunicar e intercambiar datos como, por ejemplo, configuraciones y notificaciones, además de sincronizar los datos necesarios para el correcto funcionamiento de un grupo de instancias del producto. Esto permite contar con la misma configuración del producto en todos los miembros de un clúster. ESET Mail Security admite clústeres de conmutación por error de Windows y clústeres de equilibrio de carga de red (NLB). Además, puede agregar miembros al Clúster de ESET manualmente sin necesidad de contar con un clúster de Windows concreto. Los clústeres de ESET funcionan en entornos tanto de dominio como de grupo de trabajo.
- Análisis del almacenamiento: analiza todos los archivos compartidos en un servidor local. Esta función permite analizar de forma selectiva únicamente aquellos datos del usuario que estén almacenados en el servidor de archivos.
- Instalación basada en componentes: puede elegir qué componentes desea agregar o quitar.
- Exclusiones de procesos: excluye procesos concretos del análisis de acceso del antivirus. Debido al papel esencial que realizan los servidores dedicados (el servidor de aplicaciones, el servidor de almacenamiento, etc.), es obligatorio realizar copias de seguridad periódicas para recuperarse a tiempo de incidentes graves de cualquier

tipo. Con el fin de mejorar la velocidad de la copia de seguridad, la integridad del proceso y la disponibilidad del servicio, durante la copia de seguridad se utilizan algunas técnicas que suelen entrar en conflicto con la protección antivirus a nivel de archivos. Al intentar realizar migraciones dinámicas de máquinas virtuales pueden surgir problemas similares. La única forma eficaz de evitar ambas situaciones es desactivar el software antivirus. Al excluir procesos concretos (por ejemplo los relacionados con la solución de copia de seguridad), todas las operaciones con archivos relacionadas con dicho proceso se ignoran y se consideran seguras, minimizando de este modo las interferencias con el proceso de copia de seguridad. Se recomienda tener cuidado a la hora de crear exclusiones: una herramienta de copia de seguridad que se haya excluido puede acceder a archivos infectados sin desencadenar una alerta, razón por la cual los permisos ampliados solo se autorizan en el módulo de protección en tiempo real.

- Recolector de registros de ESET: recopila automáticamente información tal como la configuración de ESET Mail Security y distintos registros. El Recolector de registros de ESET le facilitará la tarea de recopilar la información de diagnóstico necesaria para ayudar a que los técnicos de ESET resuelvan un problema rápidamente.
- eShell (ESET Shell) - eShell 2.0 ya está disponible en ESET Mail Security. eShell es una interfaz de línea de comandos que ofrece a los usuarios avanzados y a los administradores opciones más completas para la gestión de los productos de servidor de ESET.
- Análisis Hyper-V: se trata de una nueva tecnología que permite analizar discos de máquina virtual en Microsoft Hyper-V Server sin necesidad de tener ningún "Agente" instalado en la máquina virtual determinada.
- Una mejor integración con ESET Remote Administrator, incluida la capacidad de programar análisis a petición.

1.2 Páginas de Ayuda

Estimado cliente, le damos la bienvenida a ESET Mail Security. El objetivo de esta guía es ayudarle a sacar el máximo partido de ESET Mail Security.

Los temas de esta guía están divididos en diversos capítulos y subcapítulos. Puede acceder a información relevante explorando el **Contenido** de las páginas de ayuda. Igualmente, puede usar el **Índice** para explorar por palabras clave o utilizar la **Búsqueda** de texto completo.

Si desea obtener más información sobre cualquiera de las ventanas del programa, pulse F1 en el teclado mientras la ventana en cuestión se encuentra abierta. Aparecerá la página de Ayuda relacionada con la ventana que esté visualizando.

ESET Mail Security permite buscar temas de ayuda por palabra clave y escribir palabras o frases para realizar búsquedas en la Guía del usuario. La diferencia entre estos dos métodos es que una palabra clave puede estar relacionada de forma lógica con las páginas de Ayuda que no contienen esa palabra clave determinada en el texto. La búsqueda por palabras y frases se realiza en el contenido de todas las páginas y muestra únicamente las que contienen la palabra o frase buscada en el texto real.

1.3 Métodos utilizados

Para usar los métodos de correo electrónico se usan los siguientes tres métodos:

- Protección de la base de datos de buzones: anteriormente conocido como análisis del buzón de correo mediante VSAPI. Este tipo de protección solo está disponible para Microsoft Exchange Server 2010, 2007 y 2003 en funcionamiento en los roles Servidor de buzones de correo (Microsoft Exchange 2010 y 2007) o Servidor administrativo (Microsoft Exchange 2003). Este tipo de análisis puede realizarse en una instalación con un solo servidor con varios roles de Exchange Server en un ordenador (siempre que incluya el rol de buzones de correo o administrativo).
- Protección del correo electrónico: anteriormente conocido como filtrado de mensajes a nivel del servidor SMTP. Esta protección la proporciona el agente de transporte, y solo está disponible para Microsoft Exchange Server 2007 o versiones más recientes con el rol Servidor de transporte perimetral o Servidor concentrador de transporte. Este tipo de análisis puede realizarse en una instalación con un solo servidor con varios roles de Exchange Server en un ordenador (siempre que incluya uno de los roles de servidor mencionados).

- Análisis de la base de datos a petición: le permite ejecutar o programar un análisis de la base de datos de buzones de correo. Esta función solo está disponible en Microsoft Exchange Server 2007 o versiones más recientes con el rol Servidor de buzones de correo o Concentrador de transporte. Esto también se aplica a una instalación con un solo servidor con varios roles de Exchange Server en un ordenador (siempre que incluya uno de los roles de servidor mencionados). Consulte Roles de Exchange Server 2013 para acceder a información específica sobre los roles de Exchange 2013.

1.3.1 Protección de la base de datos de buzones

El proceso de análisis del buzón de correo se activa y controla con Microsoft Exchange Server. Los mensajes de correo electrónico de la base de datos de archivos de Microsoft Exchange Server se analizan constantemente. Según la versión de Microsoft Exchange Server, la versión de la interfaz de VSAPI y la configuración definida por el usuario, el proceso de análisis se puede activar en cualquiera de estas situaciones:

- Cuando el usuario accede al correo electrónico, por ejemplo, en un cliente de correo electrónico (el correo electrónico se analiza siempre con la base de firmas de virus más reciente).
- En segundo plano, cuando se hace poco uso de Microsoft Exchange Server.
- Proactivamente (de acuerdo con el algoritmo interno de Microsoft Exchange Server).

Actualmente, la interfaz de VSAPI se utiliza para el análisis antivirus y la protección basada en reglas.

1.3.2 Protección del correo electrónico

El filtrado de nivel de servidor SMTP se garantiza mediante un complemento especializado. En Microsoft Exchange Server 2000 y 2003, el complemento en cuestión (Receptor de sucesos) se registra en el servidor SMTP como parte de Internet Information Services (IIS). En Microsoft Exchange Server 2007/2010, el complemento se registra como agente de transporte en los roles Perimetral o Concentrador de Microsoft Exchange Server.

El filtrado de nivel de servidor SMTP por parte de un agente de transporte ofrece protección en forma de reglas antivirus, antispam y definidas por usuario. A diferencia del filtrado VSAPI, el filtrado de nivel de servidor SMTP se realiza antes de que el correo analizado llegue al buzón de correo de Microsoft Exchange Server.

1.3.3 Análisis de la base de datos a petición

Como la ejecución de un análisis de la base de datos de correo electrónico de un entorno de tamaño considerable puede provocar una carga del sistema no deseada, puede optar qué bases de datos y cuáles de sus buzones van a analizarse. Puede filtrar aún más los objetos de análisis al especificar la marca de hora de los mensajes que desea analizar, con el fin de minimizar la repercusión en los recursos del sistema servidor.

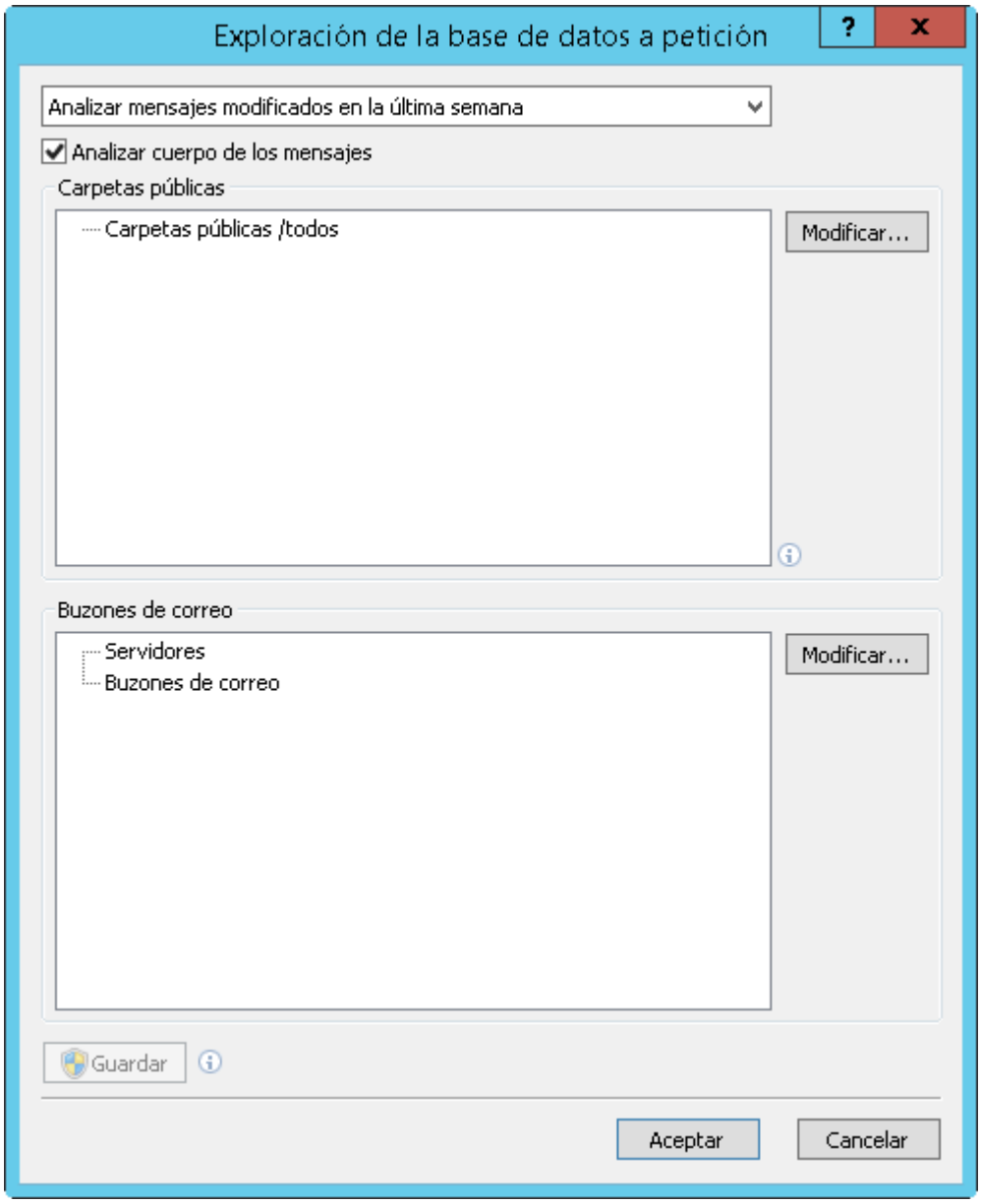
Los siguientes tipos de elemento se analizan tanto en las carpetas públicas como en los buzones de usuarios:

- Correo electrónico
- Publicación
- Elementos de calendario (reuniones/citas)
- Tareas
- Contactos
- Diario

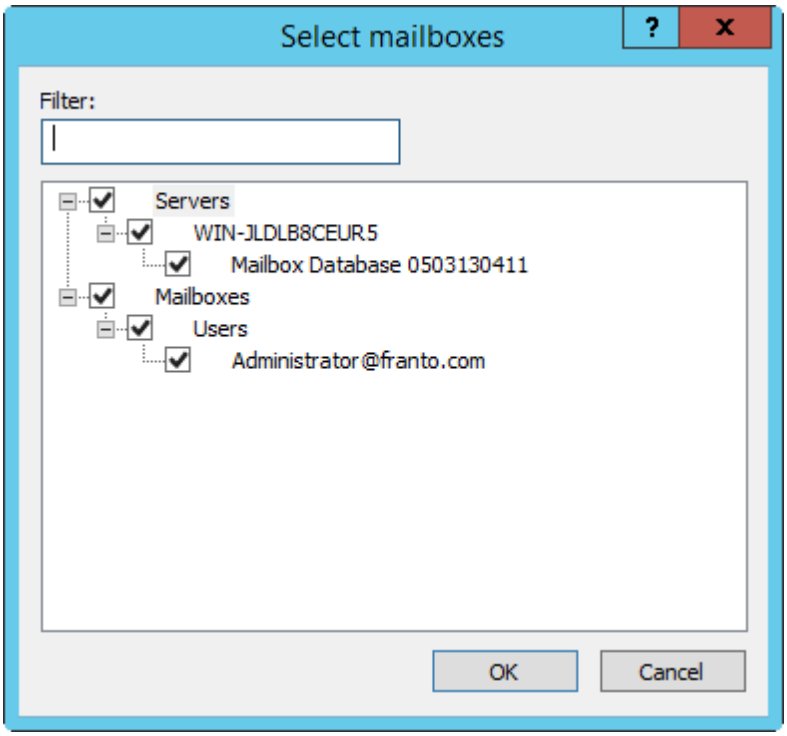
Puede usar la lista desplegable para elegir qué mensajes desea analizar según su marca de hora. Por ejemplo, los mensajes modificados durante la última semana. También puede optar por analizar todos los mensajes, en caso de ser necesario.

Active la casilla de verificación situada junto a **Analizar cuerpo de los mensajes** para activar o desactivar el análisis del cuerpo de los mensajes.

Haga clic en **Editar** para seleccionar la carpeta pública que se analizará.


Exploración de la base de datos a petición
Analizar mensajes modificados en la última semana
Analizar cuerpo de los mensajes
Carpetas públicas
Carpetas públicas /todos
Modificar...
Buzones de correo
Servidores
Buzones de correo
Modificar...
Guardar
Aceptar
Cancelar

Active las casillas de verificación situada junto a las bases de datos y buzones del servidor que desea analizar. **Filtrar** le permite encontrar bases de datos y buzones rápidamente, especialmente si su infraestructura de Exchange contiene un número elevado de buzones de correo.



Haga clic en **Guardar** para guardar los objetos y los parámetros de análisis en el perfil de análisis a petición.

1.4 Tipos de protección

Hay tres tipos de protección:

- Protección antivirus
- Protección antispam
- Aplicación de reglas definidas por el usuario

1.4.1 Protección antivirus

La protección antivirus es una de las funciones básicas de ESET Mail Security. La protección antivirus protege contra ataques maliciosos al sistema mediante el control de las comunicaciones por Internet, el correo electrónico y los archivos. Si se detecta una amenaza con código malicioso, el módulo antivirus puede bloquearla y, a continuación, desinfectarla, eliminarla o moverla a la Cuarentena.

1.4.2 Protección Antispam

La protección antispam incorpora varias tecnologías (RBL, DNSBL, identificación mediante huellas digitales, análisis de reputación, análisis de contenido, filtro Bayesiano, reglas, creación manual de listas blancas/negras, etc.) para alcanzar el máximo nivel de detección de amenazas de correo electrónico. El motor de análisis antispam genera un valor de probabilidad en forma de porcentaje (de 0 a 100) para cada mensaje de correo electrónico escaneado.

ESET Mail Security también puede usar el método de lista gris (desactivado de forma predeterminada) de filtrado del correo electrónico. Este método se basa en la especificación RFC 821, el cual indica que como SMTP se considera un transporte poco fiable, todos los agentes de transferencia de mensajes (MTA) deberían intentar entregar un mensaje de correo electrónico repetidamente cuando detecten un error de entrega temporal. Muchos mensajes de correo no deseado se entregan una vez a una lista masiva de direcciones de correo electrónico generadas automáticamente. La lista gris calcula un valor de control (hash) para la dirección del remitente del sobre, la dirección del destinatario del sobre y la dirección IP del MTA que realiza el envío. Si el servidor no encuentra el valor de control de estas tres direcciones en la base de datos, rechaza el mensaje y devuelve un código de error temporal

(por ejemplo, el error temporal 451). Un servidor legítimo intentará entregar el mensaje otra vez después de un intervalo de tiempo variable. Cuando se realiza el segundo intento, este valor de control se almacena en la base de datos de conexiones comprobadas, de manera que a partir de ese momento se entregarán todos los mensajes con las características pertinentes.

1.4.3 Aplicación de reglas definidas por el usuario

La protección basada en reglas está disponible para su análisis con el agente de transporte y VSAPI. Puede utilizar la interfaz de usuario de ESET Mail Security para crear reglas individuales que, después, puede combinar. Si una regla utiliza varias condiciones, estas se enlazarán con el operador lógico AND. De esta manera, la regla solo se ejecutará si se cumplen todas sus condiciones. Si se crean varias reglas, se aplicará el operador lógico OR, de modo que el programa ejecutará la primera regla cuyas condiciones se cumplan.

En la secuencia de análisis, la primera técnica que se utiliza es la creación de listas grises (si está activada). Los procedimientos posteriores ejecutarán siempre las siguientes técnicas: protección basada en reglas definidas por el usuario, análisis antivirus y, por último, análisis antispam.

1.5 Interfaz de usuario

El diseño de la interfaz gráfica de usuario (GUI) de ESET Mail Security pretende ser lo más intuitivo posible. La GUI proporciona a los usuarios acceso rápido y sencillo a las principales funciones del programa.

Además de la GUI principal, está disponible una ventana de **Configuración avanzada**, a la que se puede acceder desde cualquier punto del programa con solo pulsar la tecla F5.

En esta ventana puede configurar los ajustes y las opciones según sus necesidades. El menú de la izquierda está compuesto por las siguientes categorías: **Servidor**, **Ordenador**, **Actualización**, **Web y correo electrónico**, **Control de dispositivos**, **Herramientas** e **Interfaz de usuario**. Algunas de las categorías principales contienen subcategorías. Cuando hace clic en uno de los elementos (categoría o subcategoría) del menú de la izquierda, en el panel de la derecha se muestra la configuración de dicho elemento.

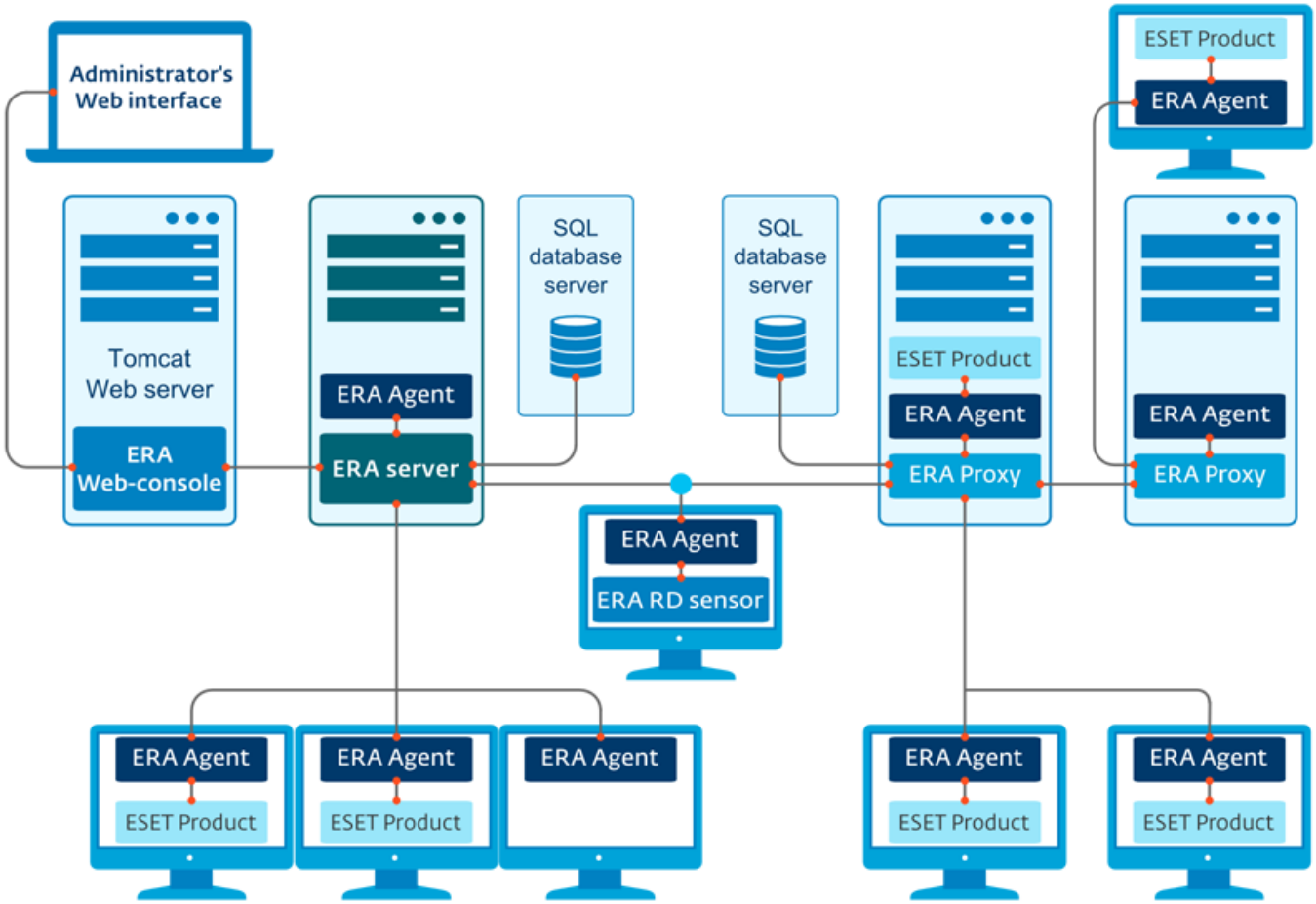
Si desea obtener más información sobre la interfaz gráfica de usuario, haga clic aquí.

1.6 Administración a través de ESET Remote Administrator

ESET Remote Administrator (ERA) es una aplicación que le permite administrar los productos de ESET en un entorno de red desde una ubicación central. El sistema de administración de tareas de ESET Remote Administrator le permite instalar soluciones de seguridad de ESET en ordenadores remotos y responder rápidamente a nuevos problemas y amenazas. ESET Remote Administrator no proporciona protección frente a código malicioso por sí solo, sino que confía en la presencia de soluciones de seguridad de ESET en cada cliente.

Las soluciones de seguridad de ESET son compatibles con redes que incluyan varios tipos de plataforma. Su red puede incluir una combinación de sistemas operativos actuales de Microsoft, Linux, OS X y sistemas operativos de dispositivos móviles (teléfonos móviles y tabletas).

En la imagen siguiente se muestra una arquitectura de ejemplo para una red protegida con soluciones de seguridad de ESET administradas mediante ERA:



NOTA: para obtener más información sobre ERA, consulte la ayuda en línea de ESET Remote Administrator.

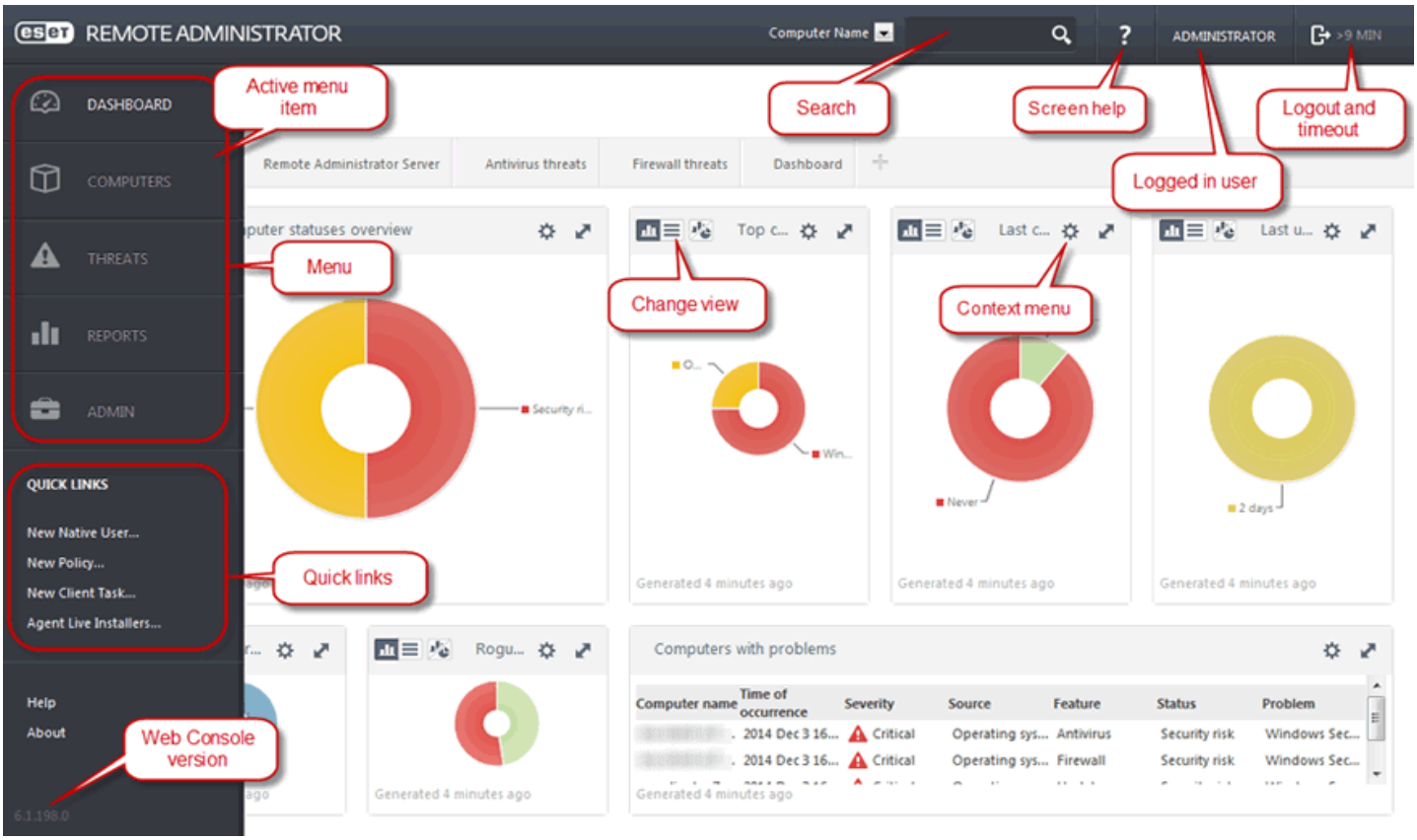
1.6.1 ERA Server

ESET Remote Administrator Server es uno de los componentes principales de ESET Remote Administrator. Es la aplicación ejecutiva que procesa todos los datos recibidos de los clientes que se conectan al servidor (a través de ERA Agent). ERA Agent facilita la comunicación entre el cliente y el servidor. Los datos (registros de clientes, configuración, replicación del agente, etc.) se almacenan en una base de datos. ERA Server necesita una conexión estable a un servidor de bases de datos para procesar los datos correctamente. Le recomendamos que instale ERA Server y la base de datos en servidores diferentes para optimizar el rendimiento. El ordenador donde se instale ERA Server debe configurarse de modo que acepte todas las conexiones de agente, proxy y sensor RD, que se verifican mediante certificados. Cuando ERA Server se instala puede abrir ERA Web Console, aplicación que se conecta al ERA Server (como se muestra en el diagrama). Al administrar las soluciones de seguridad de ESET en su red, todas las operaciones relativas a ERA Server se realizan desde la Web Console.

1.6.2 Web Console

ERA Web Console es una interfaz web de usuario que presenta datos de ERA Server y permite administrar las soluciones de seguridad ESET de su entorno. A Web Console se accede desde un navegador. Muestra información general del estado de los clientes en la red y se puede utilizar para implementar de forma remota soluciones de ESET en ordenadores no administrados. Si opta por permitir el acceso al servidor web desde Internet, dispondrá de la enorme ventaja que supone poder usar ESET Remote Administrator casi desde cualquier sitio y dispositivo que disponga de conexión a Internet activa.

Este es el tablero de Web Console:



En la barra superior de Web Console encontramos la herramienta **Búsqueda rápida**. Seleccione en el menú desplegable la opción **Nombre del ordenador**, **IPv4/Dirección IPv6** o **Nombre de la amenaza**, escriba la cadena de búsqueda en el campo de texto, y haga clic en el símbolo de la lupa o pulse **Intro** para buscar. Se le redirigirá a la sección Grupos, en la que se mostrarán los resultados de la búsqueda; un cliente o una lista de clientes. Los clientes se administran desde Web Console. Puede acceder a Web Console con los dispositivos y navegadores más habituales.

NOTA: para obtener más información, consulte la ayuda en línea de ESET Remote Administrator.

1.6.3 Agente

ERA Agent es un componente esencial de ESET Remote Administrator. Un producto de ESET instalado en un ordenador cliente (por ejemplo, ESET Endpoint Security para Windows) se comunica con ERA Server a través del agente. Esta comunicación permite la administración de los productos de ESET de todos los clientes remotos desde una ubicación central. El agente recopila información del cliente y la envía al servidor. Si el servidor envía una tarea al cliente, esta se envía al agente y este, a su vez, la envía al cliente. Toda la comunicación de la red tiene lugar entre el agente y la parte superior de la red de ERA (el servidor y el proxy).

NOTA: para obtener más información, consulte la ayuda en línea de ESET Remote Administrator.

El agente de ESET utiliza uno de estos tres métodos para conectarse al servidor:

1. El agente del cliente se conecta directamente al servidor.
2. El agente del cliente se conecta a través de un proxy que está conectado al servidor.
3. El agente del cliente se conecta al servidor a través de varios proxies.

El agente de ESET se comunica con las soluciones de ESET instaladas en un cliente, recopila información de los programas en dicho cliente y envía al cliente la información de configuración recibida del servidor.

NOTA: el proxy de ESET tiene su propio agente, que gestiona todas las tareas de comunicación entre clientes, otros proxies y el servidor.

1.6.4 Sensor RD

El **Sensor RD (Rogue Detection)** es una herramienta de búsqueda para ordenadores de la red. Este sensor forma parte de ESET Remote Administrator y se ha diseñado para la detección de máquinas en la red. Ofrece un método práctico para añadir ordenadores nuevos a ESET Remote Administrator sin tener que hacerlo manualmente. Todos los ordenadores detectados en la red se muestran en Web Console. Desde aquí puede realizar otras acciones con los ordenadores clientes individuales.

RD Sensor es un oyente pasivo que detecta los ordenadores que están presentes en la red y envía información sobre ellos a ERA Server. ERA Server, a continuación evalúa si los PC que se encuentran en la red son desconocidos o ya están administrados.

NOTA: para obtener más información, consulte la ayuda en línea de ESET Remote Administrator.

1.6.5 Proxy

ERA Proxy es otro componente de ESET Remote Administrator y tiene dos funciones. En el caso de una red de tamaño mediano o de empresa con muchos clientes (por ejemplo, 10 000 clientes o más), puede utilizar ERA Proxy para distribuir la carga entre varios servidores ERA Proxy y así reducir la carga del ERA Server principal. La otra ventaja de ERA Proxy es que lo puede utilizar cuando se conecta a una sucursal remota con un vínculo débil. Esto significa que el ERA Agent de cada cliente no se conecta directamente al ERA Server principal, sino que lo hace a través de ERA Proxy, situado en la misma red local de la sucursal. De este modo se libera el vínculo de conexión con la sucursal. El Proxy ERA acepta conexiones de todos los agentes ERA locales, suma los datos y los carga al ERA Server principal (o a otro ERA Proxy). Esto permite que la red dé cabida a más clientes sin poner en peligro el rendimiento de la red y de las consultas a la base de datos.

Según la configuración de la red, es posible que un ERA Proxy se conecte a otro ERA Proxy y, después, se conecte al ERA Server principal.

Para que ERA Proxy funcione correctamente, el ordenador host donde se instale debe tener instalado un ESET Agent y estar conectado al nivel superior (ya sea un ERA Server o un ERA Proxy superior, si lo hay) de la red.

NOTA: para acceder a un ejemplo de entorno de implementación de ERA Proxy, consulte la ayuda en línea de ESET Remote Administrator.

2. Requisitos del sistema

Sistemas operativos compatibles:

- Microsoft Windows Server 2003 SP2 (x86 y x64)
- Microsoft Windows Server 2003 R2 (x86 y x64)
- Microsoft Windows Server 2008 (x86 y x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

NOTA: la versión mínima compatible del sistema operativo es Microsoft Windows Server 2003 SP2.

Versiones compatibles de Microsoft Exchange Server:

- Microsoft Exchange Server 2003 SP1 y SP2
- Microsoft Exchange Server 2007 SP1, SP2 y SP3
- Microsoft Exchange Server 2010 SP1, SP2 y SP3
- Microsoft Exchange Server 2013 CU2, CU3, CU4 (SP1), CU5, CU6, CU7, CU8
- Microsoft Exchange Server 2016

Los requisitos de hardware dependen de la versión del sistema operativo. Recomendamos la lectura de la documentación del producto Microsoft Windows Server para obtener más información sobre los requisitos de hardware.

3. Instalación

Después de comprar ESET Mail Security, el instalador se puede descargar del sitio web de ESET (www.eset.com) como un archivo .msi.

Recuerde que el instalador debe ejecutarse con la cuenta de administrador integrado o la cuenta de administrador de dominio (en el caso de que tenga la cuenta de administrador integrado desactivada). Los demás usuarios no tienen los derechos de acceso suficientes, aunque sean miembros de un grupo de administradores. Por este motivo debe utilizar la cuenta de administrador integrado, ya que la instalación solo se puede completar con la cuenta de administrador local o de dominio.

El instalador puede ejecutarse de dos maneras:

- Puede iniciar sesión localmente con las credenciales de la cuenta de administrador y ejecutar el instalador.
- Si ha iniciado sesión con otro usuario, abra la ventana de símbolo del sistema con Ejecutar como… y escriba las credenciales de la cuenta de administrador para ejecutar el comando como dicho usuario; a continuación, escriba el comando de ejecución del instalador (p. ej. msiexec /i emsx_nt64_ENU.msi pero debe reemplazar emsx_nt64_ENU.msi por el nombre de archivo exacto del instalador msi descargado).

Tras abrir el programa de instalación y aceptar el Acuerdo de licencia para el usuario final (EULA), el asistente de instalación le guiará durante el proceso de configuración. Si decide no aceptar los términos del acuerdo de licencia, el asistente no continuará.

Completo
Este es el tipo de instalación recomendado. Con él se instalarán todas las características de ESET Mail Security. Tras elegir este tipo de instalación solo especificará las carpetas en las que desea instalar el producto, aunque también puede simplemente aceptar las carpetas de instalación predeterminadas predefinidas (opción recomendada). El programa de instalación instala todas las características del producto automáticamente.

Personalizado
El tipo de instalación Personalizado le permite elegir las características del programa de ESET Mail Security que se instalarán en el sistema. Se mostrará la lista habitual de características y componentes que selecciona para su instalación.

Además de la instalación mediante asistente puede optar por instalar ESET Mail Security de forma silenciosa a través de la línea de comandos. Este tipo de instalación no requiere ningún tipo de interacción, al igual que al usar el asistente descrito anteriormente. Es la opción perfecta para automatizar y agilizar. Este tipo de instalación recibe también el nombre de desatendida, ya que no solicita al usuario que realice acción alguna.

Instalación silenciosa/desatendida
Instalación completa desde la línea de comandos: `msiexec /i <nombre del paquete> /qn /l*xv msi.log`

NOTA: si es posible, le recomendamos encarecidamente que instale ESET Mail Security en un sistema operativo recién instalado o configurado. No obstante, si tiene que instalarlo en un sistema actual, es preferible que primero desinstale la versión anterior de ESET Mail Security, reinicie el servidor y, a continuación, instale la nueva versión de ESET Mail Security.

NOTA: si ha utilizado anteriormente otro software antivirus en el sistema, se recomienda desinstalarlo por completo antes de instalar ESET Mail Security. Para ello puede usar la herramienta ESET AV Remover, ya que facilita el proceso de desinstalación.

3.1 Pasos de instalación de ESET Mail Security

Siga los pasos indicados a continuación para instalar ESET Mail Security con el Asistente de instalación:

Instalación de ESET Mail Security
eset
MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
Bienvenido al asistente de instalación de ESET Mail Security
El asistente de instalación está preparado para instalar ESET Mail Security en su ordenador. Haga clic en Siguiente para continuar o en Cancelar para salir del asistente.
Es importante que desinstale otras aplicaciones de seguridad, como antivirus, antiespía o cortafuegos, antes de proceder con la instalación. Dichas aplicaciones podrían entrar en conflicto con este producto y provocar problemas graves.
6.2.10009.1
< Atrás
Siguiente >
Cancelar

Tras aceptar el Acuerdo de licencia para el usuario final, seleccione uno de los siguientes pasos de instalación:

- **Completo**: instala todas las características de ESET Mail Security. Este es el tipo de instalación recomendado.
- **Personalizado**: permite elegir qué características de ESET Mail Security se instalarán en el sistema.

Instalación de ESET Mail Security
Tipo de configuración
Elija el tipo de instalación que mejor se adapte a sus necesidades.
eset
Completo
Se instalarán todas las funciones del programa.
Personalizado
Elija qué funciones del programa se instalarán. Recomendado para usuarios avanzados.
< Atrás
Siguiente >
Cancelar

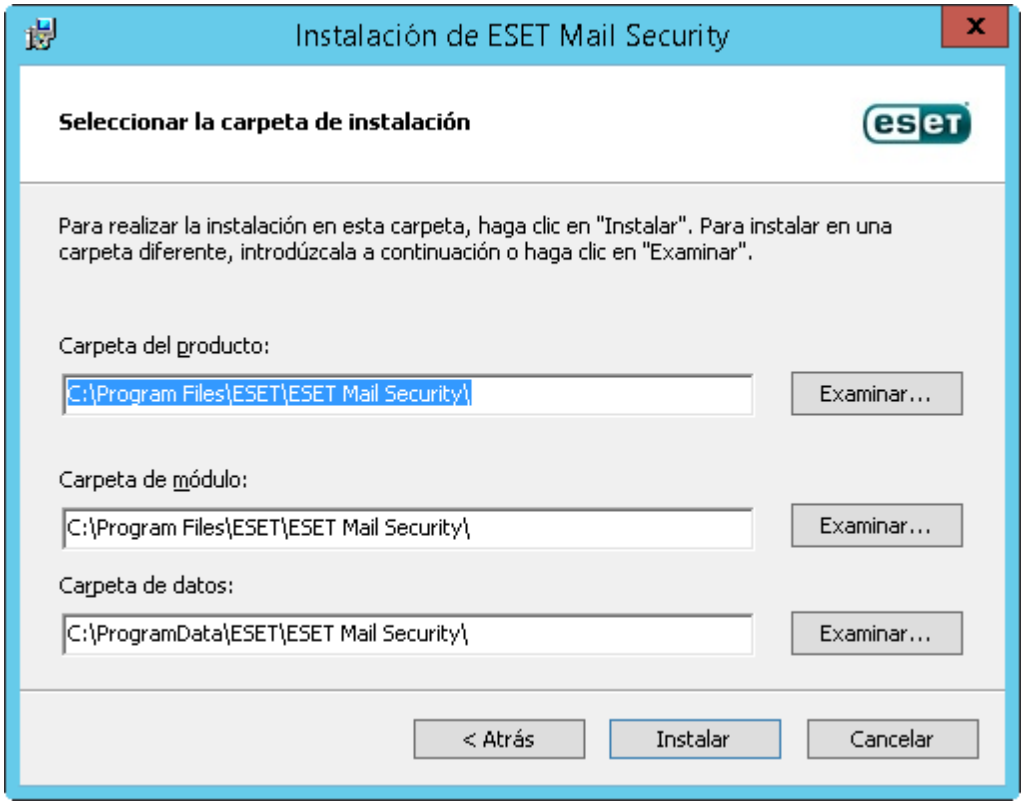
Instalación completa:

Esta instalación recibe también el nombre de instalación completa. En esta opción se instalan todos los

componentes de ESET Mail Security. Se le pedirá que seleccione la ubicación en la que se instalará ESET Mail Security. De forma predeterminada, el programa se instala en C:\Archivos de programa\ESET\ESET Mail Security. Haga clic en **Examinar** para cambiar esta ubicación (no recomendado).

NOTA: en Windows Server 2008 y Windows Server 2008 R2, la instalación del componente **Web y correo electrónico** está desactivada de forma predeterminada. Si desea instalar este componente, elija el tipo de instalación **Personalizada**.

NOTA: Si tiene previsto utilizar la Cuarentena local para los mensajes de correo electrónico y no quiere que los archivos de los mensajes en cuarentena se almacenen en su unidad `C:`, cambie la ruta de la **Carpeta de datos** a la unidad y la ubicación que desee. No obstante, debe tener en cuenta que todos los archivos de datos de ESET Mail Security se almacenarán en esta ubicación.



Instalación personalizada:

Le permite elegir las características que desea instalar. Es la opción perfecta para personalizar ESET Mail Security de forma que incluya solo los componentes necesarios.

Instalación de ESET Mail Security
Tipo de configuración
Elija el tipo de instalación que mejor se adapte a sus necesidades.
Completo
Se instalarán todas las funciones del programa.
Personalizado
Elija qué funciones del programa se instalarán. Recomendado para usuarios avanzados.
< Atrás
Siguiente >
Cancelar

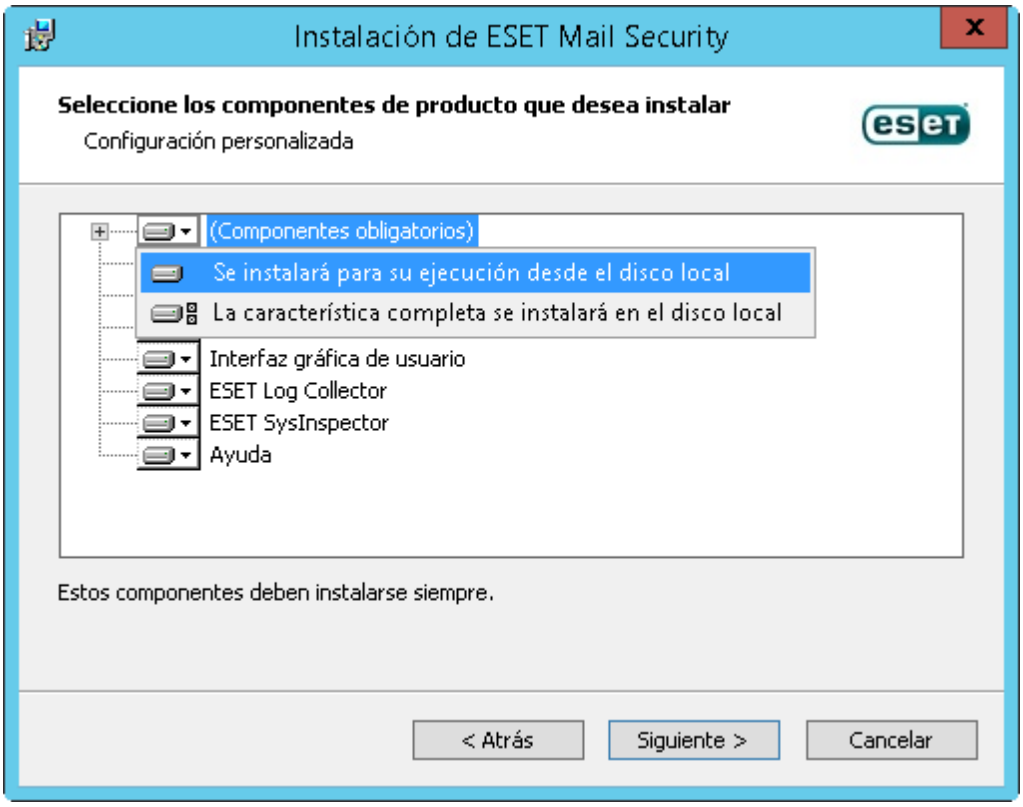
Es posible agregar o quitar componentes incluidos en la instalación. Para ello, ejecute el paquete instalador .msi que utilizó en la instalación inicial, o diríjase a **Programas y características** (disponible desde el Panel de control de Windows), haga clic con el botón derecho del ratón en ESET Mail Security y seleccione **Cambiar**. Siga los pasos indicados a continuación para agregar o quitar componentes.

Proceso para modificar (agregar o quitar) componentes, reparar la instalación y quitar o desinstalar el programa:

Hay tres opciones disponibles. Puede **Modificar** los componentes instalados, **Reparar** su instalación de ESET Mail Security o **Quitar** (desinstalar) el programa por completo.

Instalación de ESET Mail Security
Modificar, reparar o eliminar instalación
Seleccione una acción
Modificar
Agregar o elimina funciones de ESET Mail Security.
Reparar
Repara errores en el estado de instalación más reciente: corrige archivos que faltan o están dañados, accesos directos y entradas del registro.
Quitar
Elimina ESET Mail Security de su ordenador.
< Atrás
Siguiente >
Cancelar

Si elige **Modificar**, aparecerá una lista de los componentes del programa disponibles. Elija los componentes que desee agregar o quitar. Es posible agregar o quitar varios componentes al mismo tiempo. Haga clic en el componente y seleccione la opción que desee en el menú desplegable:


Instalación de ESET Mail Security
Seleccione los componentes de producto que desea instalar
Configuración personalizada
(Componentes obligatorios)
Se instalará para su ejecución desde el disco local
La característica completa se instalará en el disco local
Interfaz gráfica de usuario
ESET Log Collector
ESET SysInspector
Ayuda
Estos componentes deben instalarse siempre.
< Atrás
Siguiente >
Cancelar

Tras seleccionar una opción, haga clic en **Modificar** para efectuar las modificaciones.

NOTA: puede modificar los componentes instalados en cualquier momento con solo ejecutar el instalador. En el caso de la mayoría de los componentes, no es necesario reiniciar el servidor para efectuar el cambio. La interfaz gráfica se reiniciará y solo verá los componentes que ha elegido instalar. En el caso de los componentes que requieren un reinicio del servidor, el instalador de Windows le pedirá que reinicie y los nuevos componentes estarán disponibles cuando el servidor esté en línea de nuevo.

3.1.1 Instalación de la línea de comandos

Las siguientes opciones están pensadas para usarlas **solo para la interfaz de usuario con nivel reducido**, **básico y ninguno**. Consulte la documentación de la versión de **msiexec** utilizada para los modificadores de la línea de comandos correspondientes.

Parámetros admitidos:

APPDIR=<ruta de acceso>
- ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación de la aplicación.
- Por ejemplo: `emsx_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<ruta de acceso>
- ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación de los datos de la aplicación.

MODULEDIR=<ruta de acceso>
- ruta de acceso: ruta de acceso de un directorio válido
- Directorio de instalación del módulo.

ADDEXCLUDE=<lista>

- La lista ADDEXCLUDE es una lista separada por comas de todos los nombres de características que no se van a instalar, y sustituye a la obsoleta opción REMOVE.
- Cuando seleccione una característica para no instalarla, toda la ruta de acceso (es decir, todas sus funciones secundarias) y las funciones invisibles relacionadas deberán incluirse en la lista de forma explícita.
- Por ejemplo: `ees_nt64_ENU.msi /qn ADDEXCLUDE=Firewall,Network`

NOTA: la propiedad **ADDEXCLUDE** no se puede usar junto con **ADDLOCAL**.

ADDLOCAL=<lista>

- Instalación de componentes: lista de características no obligatorias que se pueden instalar localmente.
- Uso con los paquetes .msi de ESET: `emsx_nt64_ENU.msi /qn ADDLOCAL=<list>`
- Para obtener más información sobre la propiedad **ADDLOCAL**, consulte https://msdn.microsoft.com/es-es/library/aa367536(v=vs.85).aspx

Reglas

- La **lista ADDLOCAL** es una lista separada por comas de los nombres de todas las características que se van a instalar.
- Al seleccionar una característica para instalarla, se debe incluir en la lista y de forma explícita toda la ruta de acceso (todas las características principales).
- Consulte las reglas adicionales para obtener la información sobre el uso correcto.

Presencia de características

- **Obligatoria**: la característica se instalará siempre.
- **Opcional**: la característica puede no seleccionarse para no instalarla.
- **Invisible**: característica lógica obligatoria para que otras características funcionen correctamente.
- **Marcador de posición**: característica que no tiene repercusión en el producto, pero que debe incluirse con características secundarias.

El árbol de características es el siguiente:

Árbol de características	Nombre de la característica	Presencia de características
Ordenador	Ordenador	Obligatoria
Ordenador/Antivirus y antispyware	Antivirus	Obligatoria
Ordenador/Antivirus y antispyware > Protección del sistema de archivos en tiempo real	RealtimeProtection	Obligatoria
Ordenador/Antivirus y antispyware > Análisis del ordenador	Analizar	Obligatoria
Ordenador/Antivirus y antispyware > Protección de documentos	DocumentProtection	Opcional
Control del ordenador/dispositivo	DeviceControl	Opcional
Red	Red	Marcador de posición
Cortafuegos de red/personal	Cortafuegos	Opcional
Web y correo electrónico	WebAndEmail	Marcador de posición
Filtrado de protocolos de web y correo electrónico	ProtocolFiltering	Invisible
Protección de la web y el correo electrónico/acceso a la web	WebAccessProtection	Opcional
Protección de la web y el correo electrónico/cliente de correo electrónico	EmailClientProtection	Opcional
Protección de la web y el correo electrónico/cliente de correo electrónico/complementos de correo electrónico	MailPlugins	Invisible
Protección de la web y el correo electrónico/cliente de correo electrónico/antispam	Antispam	Opcional
Control de la web y el correo electrónico/web	WebControl	Opcional
Mirror de actualización	UpdateMirror	Opcional
Asistencia técnica de Microsoft NAP	MicrosoftNAP	Opcional

Reglas adicionales

- Si se selecciona alguna de las características de **WebAndEmail** para su instalación, la característica invisible **ProtocolFiltering** debe incluirse en la lista de forma explícita.
- Si se selecciona alguna de las características secundarias **EmailClientProtection** para su instalación, la característica invisible **MailPlugins** debe incluirse en la lista de forma explícita.

Ejemplos:

```
efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
efsw_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

Lista de propiedades CFG_:

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
• 0: desactivado, 1: activado

CFG_LIVEGRID_ENABLED=1/0
• 0: desactivado, 1: activado
• LiveGrid

FIRSTSCAN_ENABLE=1/0
• 0: desactivado, 1: activado
• Programar el primer análisis nuevo después de la instalación.

CFG_EPFW_MODE=0/1/2/3
• 0: automático, 1: interactivo, 2: política, 3: aprendizaje

CFG_PROXY_ENABLED=0/1
• 0: desactivado, 1: activado

CFG_PROXY_ADDRESS=<ip>
• Dirección IP del proxy.

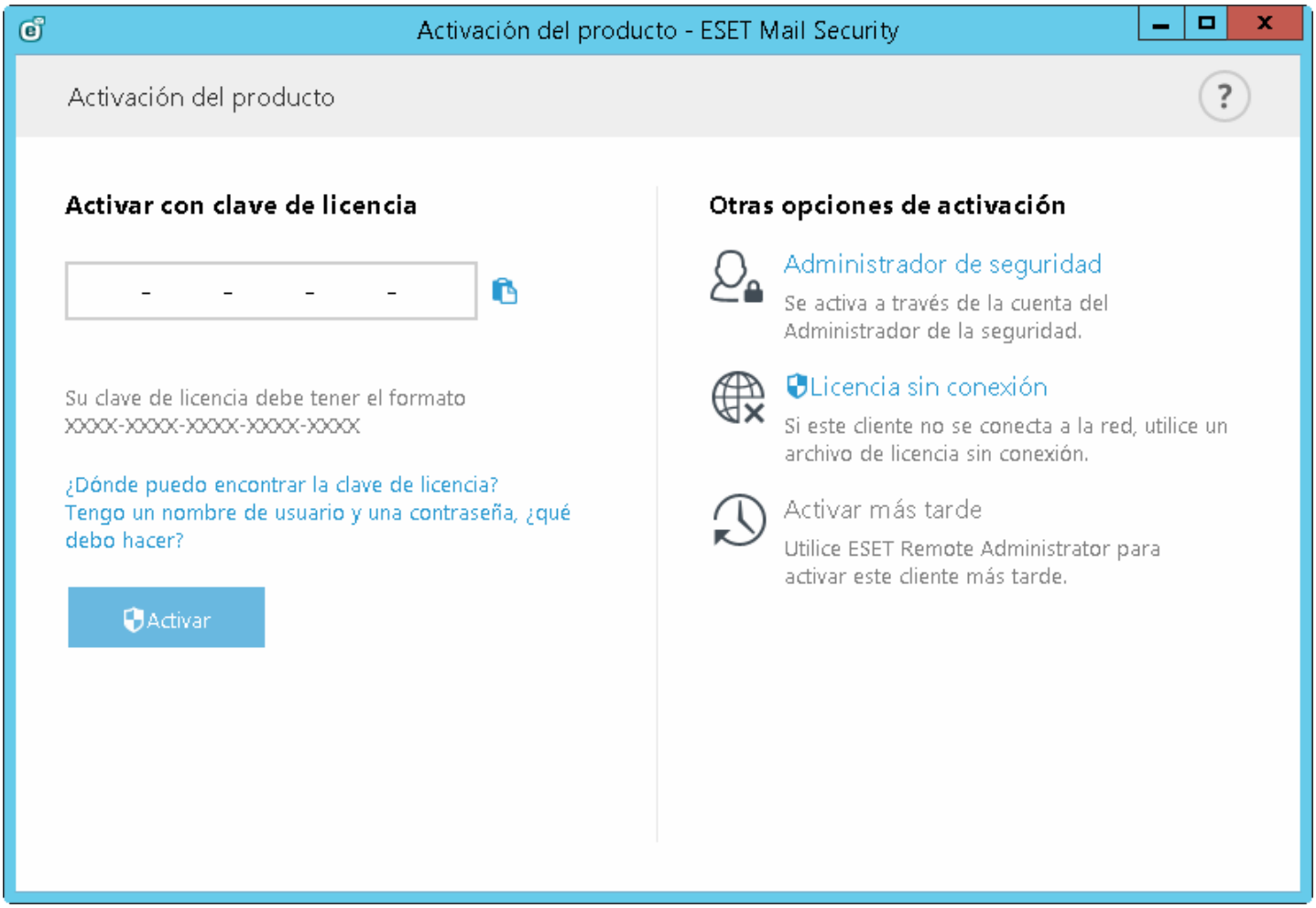
CFG_PROXY_PORT=<puerto>
• Número de puerto de proxy.

CFG_PROXY_USERNAME=<usuario>
• Nombre de usuario para autenticación.

CFG_PROXY_PASSWORD=<contraseña>
• Contraseña de autenticación.

3.2 Activación del producto

Cuando haya finalizado la instalación, se le solicitará que active el producto.


Activación del producto - ESET Mail Security
Activación del producto
Activar con clave de licencia
- - - -
Su clave de licencia debe tener el formato XXXX-XXXX-XXXX-XXXX-XXXX
¿Dónde puedo encontrar la clave de licencia?
Tengo un nombre de usuario y una contraseña, ¿qué debo hacer?
Activar
Otras opciones de activación
Administrador de seguridad
Se activa a través de la cuenta del Administrador de la seguridad.
Licencia sin conexión
Si este cliente no se conecta a la red, utilice un archivo de licencia sin conexión.
Activar más tarde
Utilice ESET Remote Administrator para activar este cliente más tarde.

Seleccione uno de los métodos disponibles para activar ESET Mail Security. Consulte Cómo activar ESET Mail Security para obtener más información.

Tras activar correctamente ESET Mail Security, se abrirá la ventana principal del programa y se mostrará el estado actual en la página Estado de la protección.

En la ventana principal del programa también se mostrarán notificaciones sobre otros elementos, como las actualizaciones del sistema (actualizaciones de Windows) o actualizaciones de la base de firmas de virus. Una vez resueltos todos aquellos elementos que requieran atención, el estado de supervisión cambiará a color verde y se mostrará el estado "**Protección máxima**".

3.3 Terminal Server

Si está instalando ESET Mail Security en un servidor Windows Server que actúa como Terminal Server, es preferible que desactive la GUI de ESET Mail Security para impedir que se inicie cada que vez que se registra un usuario. Consulte el capítulo Desactivar la GUI en Terminal Server para conocer los pasos específicos de desactivación de la GUI.

3.4 ESET AV Remover

Si desea quitar o desinstalar del sistema software antivirus de terceros, se recomienda usar ESET AV Remover. Para hacerlo, siga estos pasos:

1. Descargue ESET AV Remover de la página de descarga de utilidades del sitio web de ESET.
2. Haga clic en **Acepto, iniciar búsqueda** para aceptar el EULA y que comience la búsqueda en el sistema.
3. Haga clic en **Abrir desinstalador** para quitar el software antivirus instalado.

Si desea acceder a una lista del software antivirus de terceros que puede quitarse con ESET AV Remover, consulte este artículo de la base de conocimiento.

3.5 Actualización a una versión más reciente

Las versiones nuevas de ESET Mail Security ofrecen mejoras o solucionan problemas que no se pueden arreglar con las actualizaciones automáticas de los módulos del programa. Puede realizarse una actualización de versiones anteriores de ESET Mail Security (4.5 y anteriores) incluso si se trata de una actualización a una arquitectura diferente. Puede actualizar a una versión más reciente:

- Actualización manual mediante la descarga e instalación de una versión más reciente sobre la versión actual. Ejecute simplemente el instalador y realice una instalación normal. ESET Mail Security transferirá la configuración existente automáticamente, aunque con algunas excepciones (consulte la nota siguiente).

IMPORTANTE: existen algunas excepciones durante la actualización, no se conservarán todos los ajustes, especialmente las reglas. Esto se debe a que se ha modificado completamente la funcionalidad de las reglas en ESET Mail Security 6 con un enfoque diferente. Las reglas de las versiones anteriores de ESET Mail Security no son compatibles con las reglas de ESET Mail Security versión 6. Se recomienda configurar las reglas manualmente, también le resultará de utilidad.

A continuación, se indica una lista de ajustes que se conservan con respecto a las versiones anteriores de ESET Mail Security:

- Configuración general de ESET Mail Security.
- Ajustes de la protección frente a correo no deseado:
  - Todos los ajustes son idénticos a los de versiones anteriores, cualquier nuevo ajuste utilizará los valores predeterminados.
  - Listas blancas y listas negras.

NOTA: una vez actualizado ESET Mail Security, se recomienda revisar todos los ajustes para verificar que están correctamente configurados y cumplen sus necesidades.

3.6 Roles de Exchange Server: perimetral y concentrador

Los servidores de Transporte perimetral y de Concentrador de transporte tienen las funciones antispam desactivadas de forma predeterminada. Esta es la configuración deseada en una organización de Exchange con un servidor de Transporte perimetral. Se recomienda que el servidor Transporte perimetral donde se ejecute la protección antispam de ESET Mail Security esté configurado para filtrar los mensajes antes de que se dirijan a la organización de Exchange.

El rol perimetral es la ubicación preferida para el análisis antispam, ya que permite que ESET Mail Security rechace el correo no deseado al principio del proceso, de manera que evita poner una carga innecesaria en las capas de red. Al utilizar esta configuración, ESET Mail Security filtra los mensajes entrantes en el servidor Transporte perimetral, de modo que se pueden trasladar de forma segura al servidor Concentrador de transporte, sin necesidad de un mayor filtrado.

Sin embargo, si su organización no utiliza el servidor Transporte perimetral y solo tiene el servidor Concentrador de

transporte, se recomienda activar las características antispam en el servidor Concentrador de transporte que reciba los mensajes entrantes de Internet mediante SMTP.

3.7 Roles de Exchange Server 2013

La arquitectura de Exchange Server 2013 es diferente de las versiones anteriores de Microsoft Exchange. Desde la introducción de Exchange 2013, en la actualización acumulativa 4 (que de hecho es el SP1 para Exchange 2013) se ha incluido de nuevo el rol de servidor Transporte perimetral.

Si tiene previsto proteger Microsoft Exchange 2013 con ESET Mail Security, instálelo en un sistema que ejecute Microsoft Exchange 2013 con el rol de servidor de buzón de correo o de Transporte Perimetral.

Existe una excepción si tiene pensado instalar ESET Mail Security en Windows SBS (Small Business Server) o tiene Microsoft Exchange 2013 con varios roles en un mismo servidor. En este caso, todos los roles de Exchange se ejecutan en el mismo servidor, y por lo tanto ESET Mail Security proporcionará protección total, incluida la protección de los servidores de correo.

Si instala ESET Mail Security en un sistema en el que solo se ejecuta el rol de servidor de acceso de cliente (servidor CAS dedicado), las funciones de ESET Mail Security más importantes estarán desactivadas, especialmente las funciones de servidor de correo. En este caso, únicamente la protección del sistema de archivos en tiempo real y algunos componentes que pertenecen a Protección del ordenador serán funcionales, y por lo tanto los servidor de correo electrónico no se protegerán. Por este motivo, no se recomienda instalar ESET Mail Security en un servidor con el rol de servidor de acceso de cliente. Esto no se aplica a Windows SBS (Small Business Server) y Microsoft Exchange con varios roles en el mismo ordenador, tal como se mencionó anteriormente.

NOTA: Microsoft Exchange 2013 presenta determinadas restricciones técnicas que impiden la compatibilidad de ESET Mail Security con el rol de servidor de acceso de cliente (CAS). Esto no se aplica a la instalación de Windows SBS o Microsoft Exchange 2013 en un mismo servidor con todos los roles de servidor. En este caso puede ejecutar ESET Mail Security con el rol CAS en el servidor, ya que el servidor de buzones de correo y el de transporte perimetral están protegidos.

3.8 Protección antispam y conector POP3

Las versiones de Microsoft Windows Small Business Server (SBS) incluyen conector POP3 nativo integrado, que permite al servidor recuperar mensajes de correo electrónico desde servidores de POP3 externos. La implementación de este conector POP3 nativo de Microsoft es diferente según la versión de SBS.

es compatible con el conector POP3 de Microsoft SBS si se configura correctamente. Se analizan los mensajes descargados a través del conector POP3 de Microsoft para detectar la presencia de correo no deseado. La protección antispam para estos mensajes es posible gracias a que el conector de POP3 reenvía mensajes de correo electrónico desde una cuenta POP3 a Microsoft Exchange Server a través de SMTP.

ha sido probado con servicios de correo electrónico conocidos como **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** y **gmx.de** en los siguientes sistemas SBS:

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Small Business Server 2008
- Microsoft Windows Small Business Server 2011

IMPORTANTE: si utiliza el conector POP3 integrado de Microsoft SBS y analiza todos los mensajes de correo electrónico para detectar correo no deseado, vaya a Configuración avanzada, desplácese hasta **Servidor** > **Protección del correo electrónico** > Configuración avanzada y en el ajuste **Analizar también los mensajes procedentes de conexiones autenticadas o internas** elija **Analizar mediante la protección antivirus y antispam** en la lista desplegable. De esta manera se garantiza la protección antispam para correo electrónico recuperado desde cuentas POP3.

Puede emplear también un conector POP3 de terceros, como un P3SS (en lugar del conector POP3 integrado de Microsoft SBS). ESET Mail Security ha sido probado en los siguientes sistemas (mediante el uso de recuperación de mensajes con el conector P3SS desde **Gmail.com**, **Outlook.com**, **Yahoo.com**, **Yandex.com** y **gmx.de**):

- Microsoft Windows Small Business Server 2003 R2
- Microsoft Windows Server 2008 con Exchange Server 2007
- Microsoft Windows Server 2008 R2 con Exchange Server 2010
- Microsoft Windows Server 2012 R2 con Exchange Server 2013

4. Guía para principiantes

Este capítulo contiene una descripción general de ESET Mail Security, los principales elementos del menú, sus funciones y la configuración básica.

4.1 Interfaz de usuario

La ventana principal del programa ESET Mail Security se divide en dos secciones principales. En la ventana principal, situada a la derecha, se muestra información relativa a la opción seleccionada en el menú principal de la izquierda.

A continuación se describen las distintas secciones del menú principal:

Estado de la protección: contiene información sobre el estado de protección de ESET Mail Security, la validez de la licencia, la última actualización de la base de firmas de virus, estadísticas básicas e información del sistema.

Archivos de registro: permite acceder a archivos de registro que contienen información sobre todos los sucesos de programa importantes que han tenido lugar. Estos archivos contienen una descripción general de las amenazas detectadas, así como otros sucesos relacionados con la seguridad.

Análisis: le permite configurar e iniciar el análisis del almacenamiento, el análisis estándar, el análisis personalizado o el análisis de medios extraíbles. También se puede repetir el último análisis ejecutado.

Cuarentena de correo electrónico: permite gestionar fácilmente los correos electrónicos puestos en cuarentena. El administrador de la Cuarentena de correo electrónico es común para los tres tipos: Cuarentena local, Buzón en cuarentena y Cuarentena de MS Exchange.

Actualización: contiene información sobre la base de firmas de virus y le informa de si hay una actualización disponible. Desde esta sección también puede activarse el producto.

Configuración: aquí puede ajustar la configuración de seguridad del servidor y el ordenador.

Herramientas: contiene información adicional sobre su sistema y la protección, así como herramientas que pueden ayudarle a administrar otros aspectos de su seguridad. La sección Herramientas incluye los siguientes elementos: Procesos en ejecución, Observar actividad, Recolector de registros de ESET, Estadísticas de protección, Clúster, ESET Shell, ESET SysInspector, ESET SysRescue Live para crear un CD o USB de rescate y Tareas programadas. También puede Enviar muestra para su análisis y comprobar su Cuarentena.

Ayuda y asistencia técnica: proporciona acceso a páginas de ayuda, la base de conocimiento de ESET y otras herramientas de asistencia técnica. Incluye además enlaces desde los que abrir una solicitud de asistencia técnica para el servicio de atención al cliente e información sobre la actividad del producto.

El estado de protección que aparece en la sección **Supervisión** le informa del nivel de protección actual de su ordenador. El icono de estado verde de **Máxima protección** indica que se garantiza la protección máxima.

La ventana de estado contiene también enlaces rápidos a las funciones más usadas de ESET Mail Security, así como información sobre la última actualización.

¿Qué hacer si el programa no funciona correctamente?

Los módulos que funcionan correctamente presentan una marca de verificación de color verde. Aquellos módulos que no son totalmente funcionales presentan un símbolo de exclamación en rojo o un icono de notificación de color naranja, además de información adicional acerca del módulo en la parte superior de la ventana. También se muestra una sugerencia de solución para reparar el módulo. Para cambiar el estado de un módulo concreto, haga clic en **Configuración** en el menú principal y, a continuación, en el módulo deseado.

El icono rojo de estado indica problemas graves; no se garantiza la protección máxima del ordenador. Este icono se muestra en las siguientes situaciones:

- **Protección antivirus y antiespía desactivada**: si desea activar de nuevo la protección antivirus y antiespía, haga clic en **Activar protección en tiempo real** en el panel **Estado de la protección** o en **Activar la protección antivirus y antiespía** en el panel **Configuración** de la ventana principal del programa.
- Está utilizando una base de firmas de virus obsoleta.
- El producto no está activado.
- **Su licencia ha expirado:** esto se indica mediante el icono de estado de la protección, que se vuelve rojo. Una vez que expire la licencia, el programa no se podrá actualizar. Le recomendamos que siga las instrucciones de la ventana de alerta para renovar la licencia.

El icono naranja indica que un problema no grave del producto de ESET requiere su atención. Los posibles motivos son:

- **La protección del tráfico de Internet está desactivada**: si desea activar otra vez la protección del tráfico de Internet, haga clic en la notificación de seguridad y, a continuación, en **Activar la protección del tráfico de Internet**.
- **Su licencia expirará en breve**: esto se indica mediante el icono de estado de la protección, que muestra un signo de exclamación. Cuando expire la licencia, el programa no se podrá actualizar y el icono del estado de la protección se volverá rojo.

Si no consigue solucionar el problema con estas sugerencias, haga clic en **Ayuda y asistencia técnica** para acceder a los archivos de ayuda o realice una búsqueda en la base de conocimiento de ESET. Si necesita más ayuda, envíe una solicitud de atención al cliente de ESET. El servicio de atención al cliente de ESET responderá a sus preguntas y le ayudará a encontrar una solución rápidamente.

Para ver el **Estado de la protección**, haga clic en la primera opción del menú principal. En la ventana principal se mostrará un resumen del estado de funcionamiento de ESET Mail Security y un submenú con dos elementos: **Observar actividad** y **Estadísticas**. Seleccione uno de los dos para obtener información más detallada sobre el sistema.

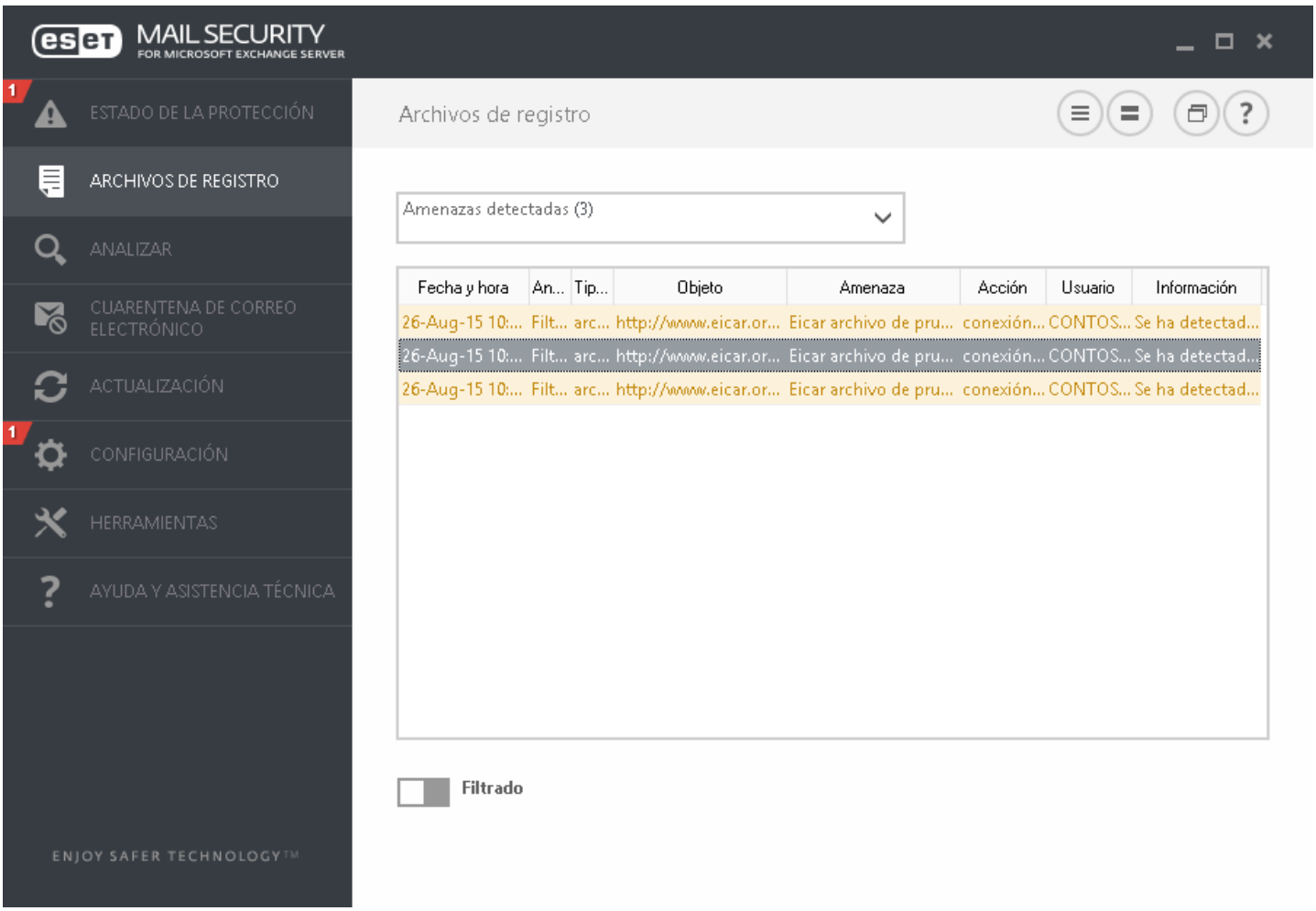
Cuando ESET Mail Security tiene todas sus funciones activas, el icono de **Estado de la protección** es de color verde. Cuando necesita atención aparece de color naranja o rojo.

Haga clic en **Observar actividad** para ver un gráfico en tiempo real de la actividad del sistema de archivos (eje horizontal). En el eje vertical se muestra la cantidad de datos leídos (línea azul) y la cantidad de datos escritos (línea roja).

En el submenú **Estadísticas** puede ver el número de objetos infectados, desinfectados y sin infectar de un módulo determinado. En la lista desplegable puede seleccionar diversos módulos.

4.2 Archivos de registro

Los archivos de registro contienen información relacionada con los sucesos importantes del programa y proporcionan información general acerca de las amenazas detectadas. Los registros constituyen una herramienta esencial en el análisis del sistema, la detección de amenazas y la resolución de problemas. Se lleva a cabo de forma activa en segundo plano, sin necesidad de que intervenga el usuario. La información se registra según la configuración de detalle de los registros. Los mensajes de texto y los registros se pueden ver directamente desde el entorno de ESET Mail Security, o exportarlos para verlos desde otra herramienta.



Se puede acceder a los archivos de registro desde la ventana principal del programa de haciendo clic en **Archivos de registro**. Seleccione el tipo de registro que desee en el menú desplegable. Están disponibles los siguientes registros:

- **Amenazas detectadas**: el registro de amenazas ofrece información detallada acerca de las amenazas detectadas por los módulos de ESET Mail Security. Incluye el momento de la detección, el nombre de la amenaza, la ubicación, la acción ejecutada y el nombre del usuario registrado en el momento en que se detectó la amenaza. Haga doble clic en la entrada del registro para ver los detalles en una ventana independiente.
- **Sucesos**: todas las acciones importantes realizadas por ESET Mail Security se registran en el registro de sucesos. El registro de sucesos contiene información sobre sucesos y errores que se produjeron en el programa. Esta opción se ha diseñado para ayudar a los administradores del sistema y los usuarios con la solución de problemas. Con frecuencia, la información aquí disponible puede ayudarle a encontrar una solución para un problema del programa.
- **Análisis del ordenador**: en esta ventana se muestran todos los resultados del análisis. Cada línea se corresponde con un control informático individual. Haga doble clic en cualquier entrada para ver los detalles del análisis correspondiente.
- **HIPS**: contiene registros de reglas específicas que se marcaron para su registro. El protocolo muestra la aplicación que invocó la operación, el resultado (si la regla se admitió o no) y el nombre de la regla creada.

- **Sitios web filtrados**: se trata de una lista de los sitios web que ha bloqueado la Protección del acceso a la Web. En estos registros puede ver la hora, la URL, el usuario y la aplicación que estableció una conexión con el sitio web determinado.
- **Control de dispositivos**: contiene registros de los dispositivos o medios extraíbles conectados al ordenador. Solo los dispositivos con una regla de control de dispositivos se registran en el archivo de registro. Si la regla no coincide con un dispositivo conectado, no se creará una entrada de registro para un dispositivo conectado. Aquí puede ver también detalles como el tipo de dispositivo, número de serie, nombre del fabricante y tamaño del medio (si está disponible).
- **Análisis de base de datos**: contiene la versión de la base de firmas de virus, la fecha, la ubicación analizada, el número de objetos analizados, el número de amenazas encontradas, el número de coincidencias con regla y la hora de finalización.
- **Protección del servidor de correo:** todos los mensajes que ESET Mail Security clasifique como spam o probable spam se registran aquí. Estos registros se aplican a los siguientes tipos de protección: Antispam, Reglas y Antivirus.
- **Creación de listas grises**: todos los mensajes evaluados con el método de listas grises se incluyen aquí.

La información mostrada en las diferentes secciones se puede copiar en el portapapeles seleccionando la entrada y haciendo clic en **Copiar** (o con el acceso directo Ctrl + C). Utilice las teclas CTRL y MAYÚS para seleccionar varias entradas.

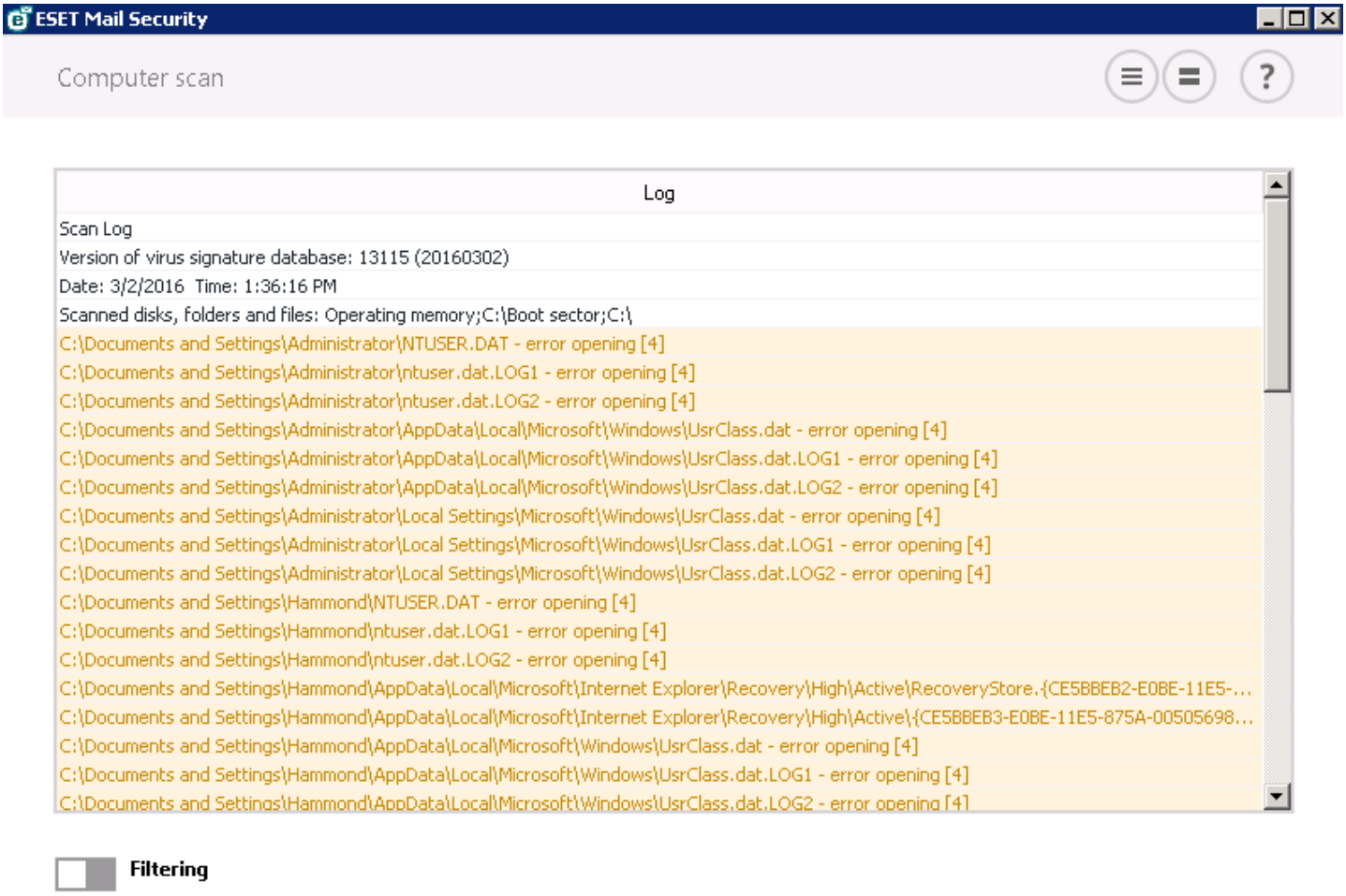
Haga clic en el icono del conmutador **Filtrado** para abrir la ventana **Filtrado de registros**, donde puede definir los criterios de filtrado.

Haga clic con el botón derecho del ratón en un registro determinado para abrir el menú contextual. En este menú contextual están disponibles las opciones siguientes:

- **Mostrar**: muestra información detallada sobre el registro seleccionado en una ventana nueva (igual que el doble clic).
- **Filtrar los mismos registros**: esta opción activa el filtrado de registros y muestra solo los registros del mismo tipo que el seleccionado.
- **Filtro...**: después de hacer clic en esta opción, en la ventana Filtrado de registros podrá definir los criterios de filtrado para entradas de registro específicas.
- **Activar filtro**: activa la configuración del filtro. La primera vez que filtra registros debe definir los criterios de filtrado. Cuando los filtros se definan, permanecerán sin cambios hasta que los edite.
- **Copiar**: copia al portapapeles la información de los registros seleccionados o resaltados.
- **Copiar todo**: copia información de todos los registros de la ventana.
- **Eliminar**: elimina los registros seleccionados o resaltados; esta acción requiere privilegios de administrador.
- **Eliminar todos**: elimina todos los registros de la ventana; esta acción requiere privilegios de administrador.
- **Exportar...**: exporta la información de los registros seleccionados o resaltados a un archivo XML.
- Exportar todo... : exporta toda la información de la ventana a un archivo XML.
- **Buscar...**: abre la ventana Buscar en el registro y le permite definir los criterios de búsqueda. Funciona con contenido que ya se ha filtrado, como una forma adicional de limitar los resultados.
- **Buscar siguiente**: busca la siguiente instancia de una búsqueda anteriormente definida (arriba).
- **Buscar anterior**: busca la instancia anterior de una búsqueda anteriormente definida (arriba).
- **Eliminar registros de diagnóstico**: elimina todos los registros de diagnóstico de la ventana.
- **Desplazar registro**: deje esta opción activada para desplazarse automáticamente por los registros antiguos y ver los registros activos en la ventana **Archivos de registro**.

4.2.1 Registro del análisis

En la ventana de registro del análisis se muestra el estado actual del análisis e información sobre el número de archivos en los que se ha detectado código malicioso.


ESET Mail Security
Computer scan
Log
Scan Log
Version of virus signature database: 13115 (20160302)
Date: 3/2/2016 Time: 1:36:16 PM
Scanned disks, folders and files: Operating memory;C:\Boot sector;C:\
C:\Documents and Settings\Administrator\NTUSER.DAT - error opening [4]
C:\Documents and Settings\Administrator\ntuser.dat.LOG1 - error opening [4]
C:\Documents and Settings\Administrator\ntuser.dat.LOG2 - error opening [4]
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat - error opening [4]
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1 - error opening [4]
C:\Documents and Settings\Administrator\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2 - error opening [4]
C:\Documents and Settings\Administrator\Local Settings\Microsoft\Windows\UsrClass.dat - error opening [4]
C:\Documents and Settings\Administrator\Local Settings\Microsoft\Windows\UsrClass.dat.LOG1 - error opening [4]
C:\Documents and Settings\Administrator\Local Settings\Microsoft\Windows\UsrClass.dat.LOG2 - error opening [4]
C:\Documents and Settings\Hammond\NTUSER.DAT - error opening [4]
C:\Documents and Settings\Hammond\ntuser.dat.LOG1 - error opening [4]
C:\Documents and Settings\Hammond\ntuser.dat.LOG2 - error opening [4]
C:\Documents and Settings\Hammond\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{CE5BBEB2-E0BE-11E5-...
C:\Documents and Settings\Hammond\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{CE5BBEB3-E0BE-11E5-875A-00505698...
C:\Documents and Settings\Hammond\AppData\Local\Microsoft\Windows\UsrClass.dat - error opening [4]
C:\Documents and Settings\Hammond\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1 - error opening [4]
C:\Documents and Settings\Hammond\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2 - error opening [4]
Filtering

La información mostrada en las diferentes secciones se puede copiar en el portapapeles seleccionando la entrada y haciendo clic en **Copiar** (o con el acceso directo Ctrl + C). Utilice las teclas CTRL y MAYÚS para seleccionar varias entradas.

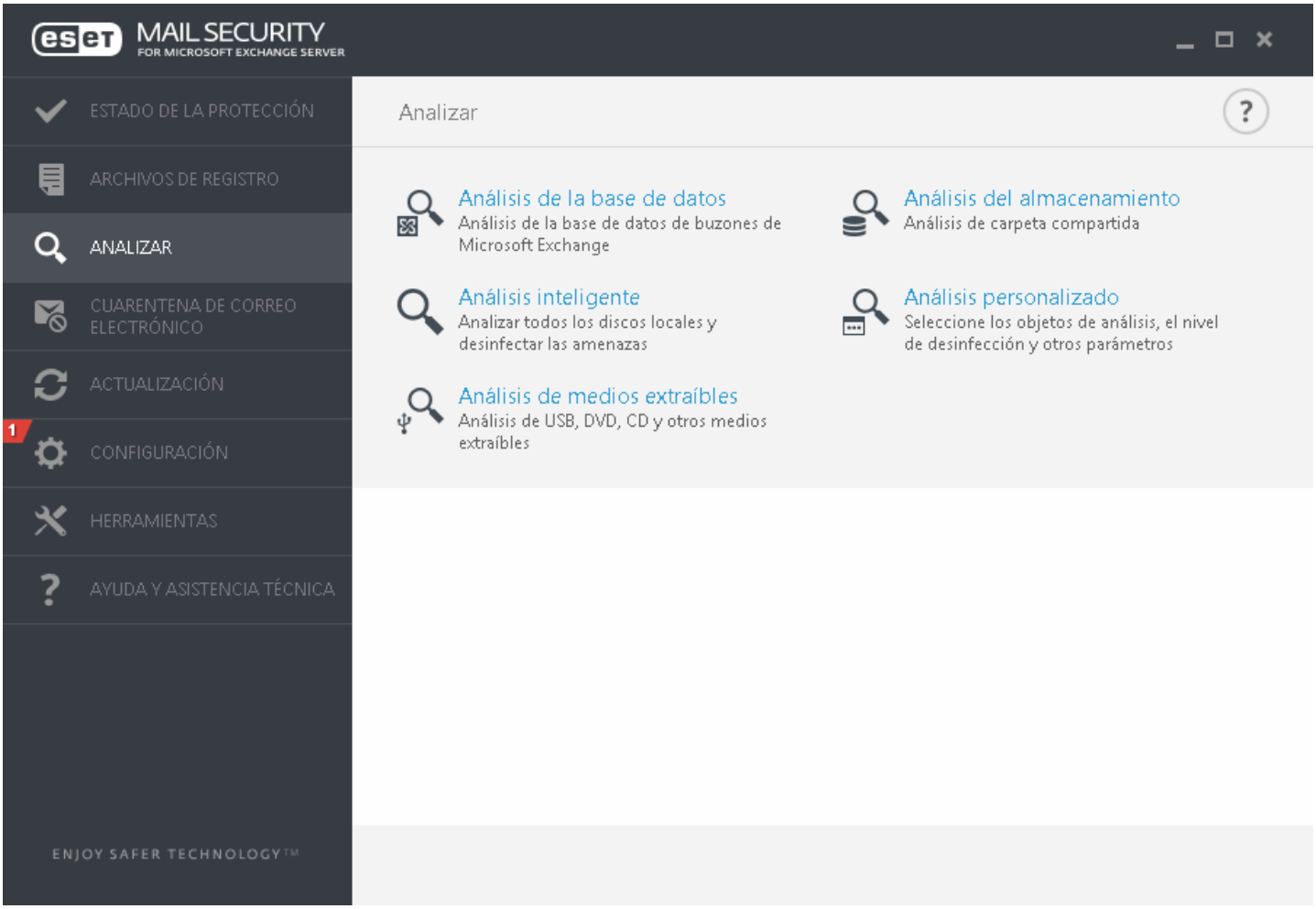
Haga clic en el icono del conmutador **Filtrado** para abrir la ventana **Filtrado de registros**, donde puede definir los criterios de filtrado.

Haga clic con el botón derecho del ratón en un registro determinado para abrir el menú contextual. En este menú contextual están disponibles las opciones siguientes:

- **Filtrar los mismos registros**: esta opción activa el filtrado de registros y muestra solo los registros del mismo tipo que el seleccionado.
- **Filtrar...**: después de hacer clic en esta opción, en la ventana Filtrado de registros podrá definir los criterios de filtrado para entradas de registro específicas.
- **Activar filtro**: activa la configuración del filtro. La primera vez que filtra registros debe definir los criterios de filtrado. Cuando los filtros se definan, permanecerán sin cambios hasta que los edite.
- **Desactivar filtro**: desactiva el filtrado (tiene el mismo efecto que hacer clic en el conmutador de la parte inferior). Esta opción solo está disponible cuando el filtrado se encuentra activado.
- **Copiar**: copia al portapapeles la información de los registros seleccionados o resaltados.
- **Copiar todo**: copia información de todos los registros de la ventana.
- **Exportar...**: exporta la información de los registros seleccionados o resaltados a un archivo XML.
- **Exportar todo...** : exporta toda la información de la ventana a un archivo XML.
- **Buscar...**: abre la ventana Buscar en el registro y le permite definir los criterios de búsqueda. Funciona con contenido que ya se ha filtrado, como una forma adicional de limitar los resultados.
- **Buscar siguiente**: busca la siguiente instancia de una búsqueda anteriormente definida (arriba).
- **Buscar anterior**: busca la instancia anterior de una búsqueda anteriormente definida (arriba).

4.3 Análisis

El análisis a petición es una parte importante de ESET Mail Security. Se utiliza para realizar análisis de archivos y carpetas en su ordenador. Desde el punto de vista de la seguridad, es esencial que los análisis del ordenador no se ejecuten únicamente cuando se sospecha que existe una infección, sino que se realicen periódicamente como parte de las medidas de seguridad rutinarias. Le recomendamos que realice un análisis en profundidad de su sistema periódicamente (por ejemplo, una vez al mes) para detectar virus que la Protección del sistema de archivos en tiempo real no haya detectado. Este fallo puede deberse a que la protección del sistema de archivos en tiempo real no estaba activada en ese momento, a que la base de firmas de virus estaba obsoleta o a que el archivo no se detectó como un virus cuando se guardó en el disco.


MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
ESTADO DE LA PROTECCIÓN
ARCHIVOS DE REGISTRO
ANALIZAR
CUARENTENA DE CORREO ELECTRÓNICO
ACTUALIZACIÓN
CONFIGURACIÓN
HERRAMIENTAS
AYUDA Y ASISTENCIA TÉCNICA
ENJOY SAFER TECHNOLOGY™
Analizar
Análisis de la base de datos
Análisis de la base de datos de buzones de Microsoft Exchange
Análisis del almacenamiento
Análisis de carpeta compartida
Análisis inteligente
Analizar todos los discos locales y desinfectar las amenazas
Análisis personalizado
Seleccione los objetos de análisis, el nivel de desinfección y otros parámetros
Análisis de medios extraíbles
Análisis de USB, DVD, CD y otros medios extraíbles

Están disponibles dos tipos de **Análisis del ordenador**. El **Análisis estándar** analiza el sistema rápidamente, sin necesidad de realizar una configuración adicional de los parámetros de análisis. El **Análisis personalizado** le permite seleccionar perfiles de análisis predefinidos y definir objetos de análisis específicos.

Consulte Progreso del análisis para obtener más información sobre el proceso de análisis.

Database scan

Lets you run On-demand database scan. You can choose **Public folders, Mail Servers and Mailboxes** to scan. Also, you can use Planificador de tareas to run the database scan at a specific time or at an event.

NOTE: If you are running Microsoft Exchange Server 2007 or 2010 you can choose between Protección de la base de datos de buzones and Análisis de la base de datos a petición. However, only one protection type out of these two can be active at a time. If you decide to use On-demand database scan you'll need to disable integration of Mailbox database protection in Advanced setup under Servidor. Otherwise On-demand **database scan** will not be available.

Análisis del almacenamiento

Analiza todas las carpetas compartidas del servidor local. Si el **Análisis del almacenamiento** no está disponible, en el

servidor no hay carpetas compartidas.

Análisis Hyper-V

Esta opción está visible en el menú solo si el Administrador de Hyper-V está instalado en el servidor que ejecuta ESET Mail Security. El análisis Hyper-V permite analizar discos de máquina virtual en Microsoft Hyper-V Server sin necesidad de tener ningún "Agente" instalado en la máquina virtual determinada. Consulte Análisis Hyper-V para obtener más información (incluida la lista de sistemas operativos host admitidos y las limitaciones).

Análisis estándar

El análisis estándar le permite iniciar rápidamente un análisis del ordenador y desinfectar los archivos infectados sin la intervención del usuario. La ventaja de este tipo de análisis es su sencillo funcionamiento, sin configuraciones de análisis detalladas. El análisis estándar comprueba todos los archivos de los discos locales y desinfecta o elimina automáticamente las amenazas detectadas. El nivel de desinfección se establece automáticamente en el valor predeterminado. Para obtener más información detallada sobre los tipos de desinfección, consulte Desinfección.

Análisis personalizado

El análisis personalizado es una solución óptima para especificar parámetros de análisis como, por ejemplo, objetos y métodos de análisis. La ventaja del análisis personalizado es su capacidad para configurar los parámetros detalladamente. Las diferentes configuraciones se pueden guardar en perfiles de análisis definidos por el usuario, que pueden resultar útiles si el análisis se realiza varias veces con los mismos parámetros.

Para seleccionar objetos de análisis, seleccione **Análisis del ordenador** > **Análisis personalizado** y elija una opción en el menú desplegable **Explorar objetivos**, o seleccione objetos específicos en la estructura de árbol. Los objetos de análisis también se pueden especificar introduciendo la ruta a la carpeta o los archivos que se desean incluir en el análisis. Si únicamente quiere analizar el sistema, sin realizar acciones de desinfección adicionales, seleccione **Analizar sin desinfectar**. Cuando vaya a realizar un análisis, haga clic en **Configuración** > **Parámetros de ThreatSense** > **Desinfección** para elegir uno de los tres niveles de desinfección.

Los análisis del ordenador en el modo personalizado solo están recomendados para usuarios avanzados que tienen experiencia previa con programas antivirus.

Análisis de medios extraíbles

Al igual que el análisis estándar, inicia rápidamente el análisis de medios extraíbles (como CD/DVD/USB) que están conectados al ordenador. Esto puede resultar útil cuando conecta una unidad flash USB a un ordenador y desea analizar su contenido por si contiene código malicioso u otras posibles amenazas.

Este tipo de análisis también se puede iniciar haciendo clic en **Análisis personalizado**, en **Medios extraíbles** en el menú desplegable **Objetos del análisis** y, a continuación, en **Analizar**.

Repetir el último análisis

Ejecuta el último análisis, sea cual fuere (de almacenamiento, estándar, personalizado, etc.), con los mismos parámetros.

NOTA: la repetición de la última función de análisis no estará disponible si está presente el Análisis de la base de datos a petición.

NOTA: le recomendamos que ejecute un análisis del ordenador una vez al mes como mínimo. El análisis se puede configurar como una tarea programada en **Herramientas** > **Tareas programadas**.

4.3.1 Análisis Hyper-V

El análisis antivirus Hyper-V ofrece la capacidad de analizar los discos de un Microsoft Hyper-V Server; es decir, una máquina virtual, sin necesidad de tener ningún agente instalado en la máquina virtual determinada. El antivirus se instala mediante los privilegios de administrador del servidor Hyper-V.

El análisis Hyper-V se deriva del módulo de análisis del ordenador a petición, aunque algunas funciones no se implementaron (análisis de memoria operativa).

Sistemas operativos host compatibles

- Windows Server 2008 R2: las máquinas virtuales solo se pueden analizar cuando están desconectadas
- Windows Server 2012
- Windows Server 2012 R2

Requisitos de hardware

El servidor no debería experimentar ningún problema de rendimiento ejecutando máquinas virtuales. El propio análisis utiliza principalmente recursos de la CPU exclusivamente.
En caso de análisis de máquinas virtuales conectadas, se requiere espacio libre en disco. El espacio libre en disco (disponible para el uso) debe duplicar al menos el espacio utilizado por los puntos de comprobación/las instantáneas y los discos virtuales.

Limitaciones concretas

- El análisis en almacenamiento RAID, volúmenes distribuidos y discos dinámicos no se admite debido a la naturaleza de los discos dinámicos. Por ello, le recomendamos que, siempre que sea posible, evite utilizar el tipo de disco dinámico en sus máquinas virtuales.
- El análisis se realiza siempre en la máquina virtual actual exclusivamente, no afecta a sus puntos de comprobación ni a sus instantáneas.
- Actualmente, ESET Mail Security no es compatible con Hyper-V en ejecución en un host de un clúster.
- Las máquinas virtuales de un host Hyper-V que se ejecutan en Windows Server 2008 R2 solo se pueden analizar en el modo de solo lectura (**Sin desinfección**), sea cual sea el nivel de desinfección seleccionado en los Parámetros de ThreatSense.

NOTA: ESET Mail Security es compatible con el análisis del MBR del disco virtual, pero se trata de un análisis de solo lectura. El análisis del MBR se realiza de forma predeterminada. Este ajuste puede modificarse en **Configuración avanzada** > **Antivirus** > **Análisis Hyper-V** > Parámetros de ThreatSense > **Sectores de inicio**.

La máquina virtual a analizar está fuera de línea (desconectada)

ESET Mail Security utiliza la administración de Hyper-V para detectar y conectarse a los discos virtuales de las máquinas virtuales. De esta forma, ESET Mail Security dispone del mismo acceso al contenido de los discos virtuales que si accediera a los datos y a los archivos de cualquier unidad genérica.

La máquina virtual a analizar está fuera de línea: **En ejecución**, **En pausa**, **Guardada**

ESET Mail Security utiliza la administración de Hyper-V para detectar los discos virtuales de las máquinas virtuales. No es posible conectarse a estos discos. Por ello, ESET Mail Security crea un punto de control o una instantánea de la máquina virtual, y luego se conecta al punto de control o la instantánea. El punto de control o la instantánea se eliminan una vez finalizado el análisis. Esto significa que el análisis de solo lectura puede realizarse, ya que la máquina virtual, que se encuentra conectada, no sufre modificaciones. Esta opción resulta útil para obtener una visión general de si hay elementos infectados en las máquinas virtuales que están en ejecución y obtener información detallada sobre dichas infecciones, en caso de haber alguna.

La creación de un punto de control o una instantánea es una operación lenta y puede requerir desde algunos segundos hasta un minuto. Debe tener esto en cuenta a la hora de planificar la ejecución de Hyper-V en un número elevado de máquinas virtuales.

Convención de nomenclatura

El módulo del análisis Hyper-V cumple la siguiente convención de nomenclatura:
`NombreMáquinaVirtual\DiscoX\VolumenY`

donde X es el número de disco e Y es el número de volumen.
Por ejemplo: `"Ordenador\Disco0\Volumen1"`.

El sufijo numérico se añade en función del orden de detección, que es idéntico al orden observado en el Administrador de discos de la máquina virtual.
Esta convención de nomenclatura se utiliza en la lista de objetivos estructurada en árbol para analizar, en la barra de progreso y también en los archivos de registro.

Ejecución de un análisis

Existen 3 alternativas para ejecutar un análisis:

- A petición: si hace clic en la opción Análisis Hyper-V en el menú de ESET Mail Security, puede ver una lista de máquinas virtuales disponibles (si hay) para analizar. Se trata de una lista estructurada en árbol en la que la entidad de menor nivel para analizar es el volumen; es decir, no se puede seleccionar un directorio o archivo para analizar, sino que al menos debe analizarse el volumen completo.
  Para enumerar los volúmenes disponibles, es necesario conectarse a los discos virtuales determinados; esto puede requerir algunos segundos. Por lo tanto, una opción más rápida es marcar una máquina virtual o sus discos para analizar.
  Tras marcar las máquinas virtuales, discos o volúmenes para analizar, haga clic en el botón Analizar.
- Mediante el programador
- A través de ERA como una tarea de cliente denominada Análisis del servidor. El elemento de menor nivel para analizar es un disco de una máquina virtual.

Pueden ejecutarse varios análisis Hyper-V simultáneamente.

Tras finalizar el análisis, se muestra una notificación sobre el mismo y un vínculo Mostrar registro que permite revisar los detalles del análisis realizado. Todos los registros de análisis están disponibles en la sección Archivos de registro de ESET Mail Security, aunque debe elegir Análisis Hyper-V en el menú desplegable para ver los registros relacionados.

Posibles problemas

- Al ejecutar el análisis de una máquina virtual conectada, debe crearse un punto de control o unainstantánea de la máquina virtual determinada y, durante la creación de un punto de control o una instantánea, ciertas acciones genéricas de la máquina virtual pueden estar limitadas o desactivadas.
- Si se desea analizar una máquina virtual desconectada, no puede encenderla hasta que finalice el análisis.
- El Administrador de Hyper-V permite nombrar dos máquinas virtuales diferentes de forma idéntica y esto plantea un problema al intentar diferenciar las máquinas mientras se revisan los registros de análisis.

4.4 Cuarentena de correo electrónico

El administrador de la cuarentena de correo electrónico está disponible para los tres tipos de cuarentena:

- Cuarentena local
- Buzón en cuarentena
- Cuarentena de MS Exchange

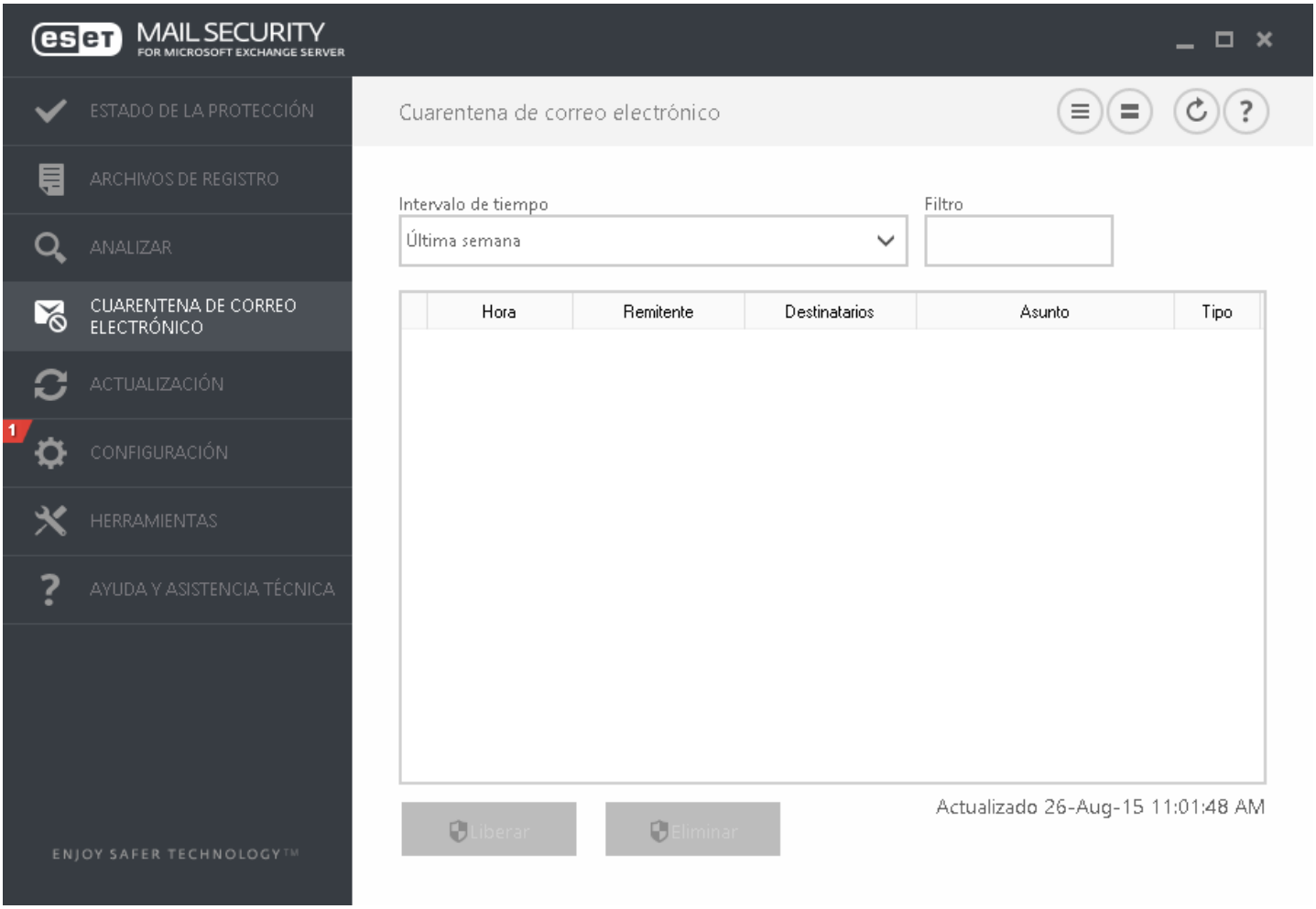
NOTA: la interfaz web de la cuarentena de correo electrónico es una alternativa al administrador de la cuarentena de correo electrónico que le permite gestionar los objetos de correo electrónico puestos en cuarentena.

Filtrado

- **Intervalo de tiempo**: puede seleccionar el intervalo de tiempo desde el que se muestran los correos electrónicos (1 semana, de forma predeterminada). Cuando cambia el intervalo de tiempo, los elementos de la cuarentena de correo electrónico se cargan de nuevo automáticamente.
- **Filtrar**: puede usar el cuadro de texto de filtrado para filtrar los correos electrónicos mostrados (se realiza la búsqueda en todas las columnas).

NOTA: los datos del administrador de la cuarentena de correo electrónico no se actualizan automáticamente; le

recomendamos que haga clic en actualizar periódicamente para ver los elementos más actualizados de la cuarentena de correo electrónico.

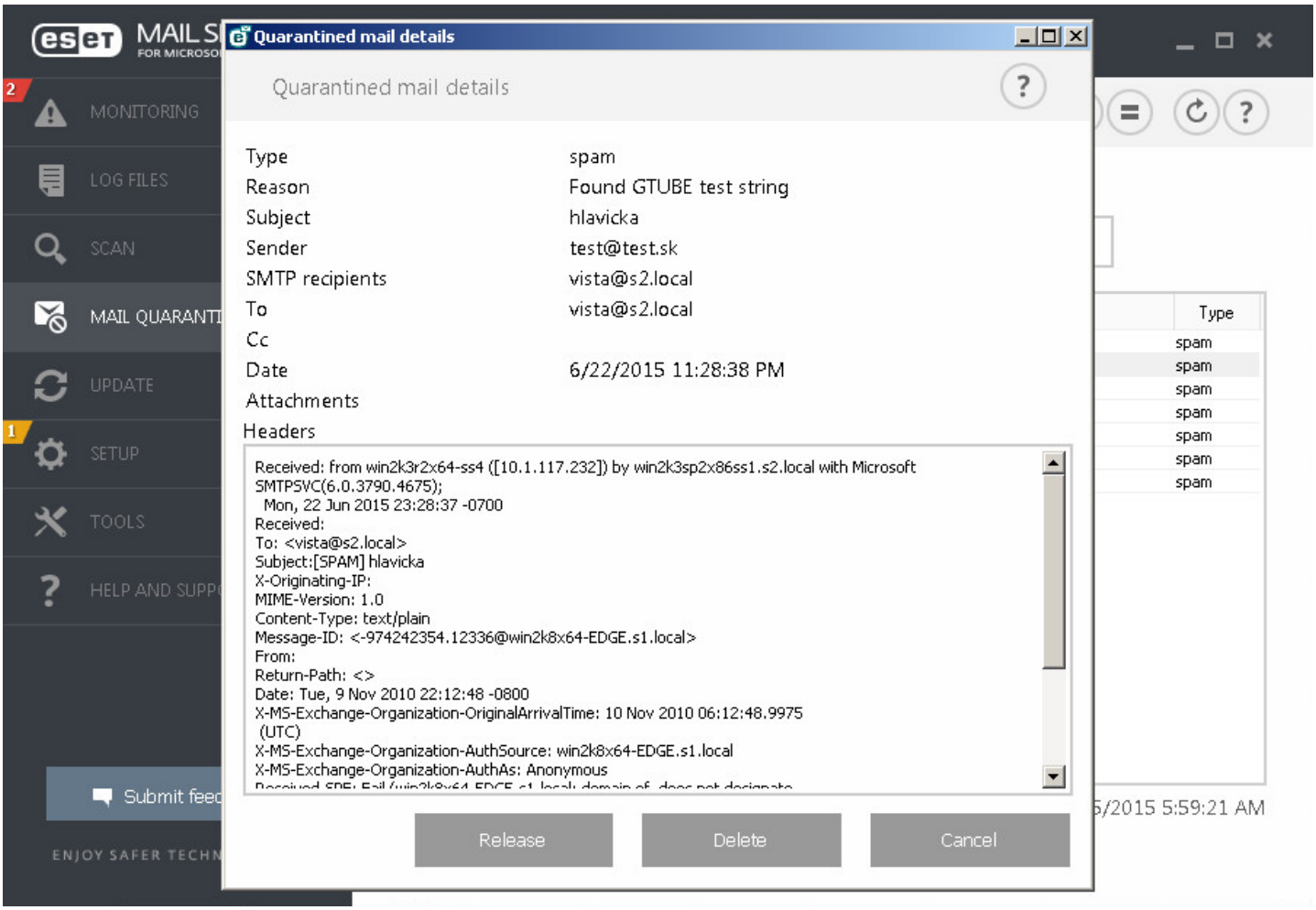


Acción

- **Liberar**: libera el correo electrónico hacia sus destinatarios originales utilizando el directorio de retransmisión, y lo elimina de la cuarentena. Haga clic en **Sí** para confirmar la acción.
- **Eliminar**: elimina el elemento de la cuarentena. Haga clic en **Sí** para confirmar la acción.

Detalles del correo electrónico en cuarentena: haga doble clic en el mensaje puesto en cuarentena, o haga clic con el botón derecho y seleccione **Detalles** y se abrirá una ventana emergente con detalles sobre el correo electrónico puesto en cuarentena Puede encontrar también información adicional sobre el correo electrónico en el encabezado de correo electrónico RFC.

Estas acciones también están disponibles en el menú contextual. Si lo desea, haga clic en **Liberar**, **Eliminar** o **Eliminar permanentemente** para realizar una acción con un mensaje de correo electrónico puesto en cuarentena. Haga clic en **Sí** para confirmar la acción. Si elige **Eliminar permanentemente**, el mensaje se eliminará también del sistema de archivos, a diferencia de **Eliminar**, acción que eliminará el elemento de la vista del administrador de la cuarentena de correo electrónico.



4.4.1 Detalles del correo electrónico en cuarentena

Esta ventana contiene información sobre el mensaje de correo electrónico en cuarentena, como **Tipo**, **Motivo**, **Asunto**, **Remitente**, **Destinatarios SMTP**, **Para**, **Cc**, **Fecha**, **Adjuntos** y **Encabezados**. Puede seleccionar, copiar y pegar los encabezados en caso necesario.

Puede adoptar una acción con el mensaje de correo electrónico en cuarentena mediante los botones:

- **Liberar**: libera el correo electrónico hacia sus destinatarios originales utilizando el directorio de retransmisión, y lo elimina de la cuarentena. Haga clic en **Sí** para confirmar la acción.
- **Eliminar**: elimina el elemento de la cuarentena. Haga clic en **Sí** para confirmar la acción.

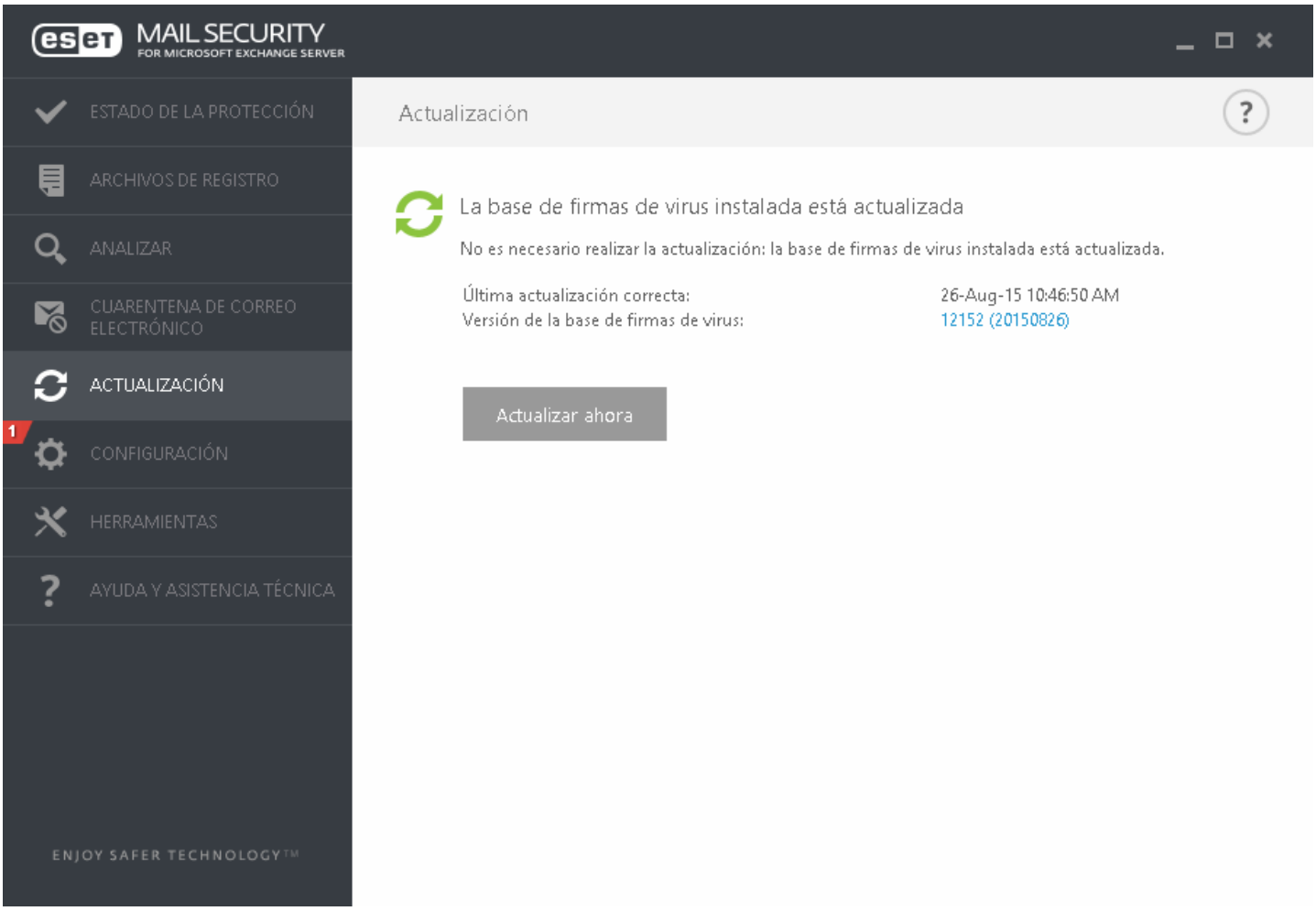
Al hacer clic en el botón **Cancelar** se cerrará la ventana Detalles del correo electrónico en cuarentena.

4.5 Actualización

La mejor manera de mantener el máximo nivel de seguridad en el ordenador es actualizar ESET Mail Security de forma periódica. El módulo Actualización garantiza que el programa está siempre actualizado de dos maneras: actualizando la base de firmas de virus y los componentes del sistema.

Haga clic en **Actualización** en la ventana principal del programa para comprobar el estado de la actualización, la fecha y la hora de la última actualización, y si es necesario actualizar el programa. La ventana principal también indica la versión de la base de firmas de virus. Esta indicación numérica es un enlace activo al sitio web de ESET, donde se muestran todas las firmas agregadas a la actualización correspondiente.

Haga clic en **Actualizar ahora** para iniciar el proceso de actualización. La actualización de la base de firmas de virus y la actualización de componentes del programa son partes importantes a la hora de mantener una protección completa frente a código malicioso.



Última actualización correcta: fecha de la última actualización. Asegúrese de que hace referencia a una fecha reciente, lo que significa que la base de firmas de virus es actual.

Versión de la base de firmas de virus: número de la base de firmas de virus, que también es un vínculo activo al sitio web de ESET. Haga clic en esta opción para ver una lista de todas las firmas agregadas en una actualización determinada.

Proceso de actualización

Tras hacer clic en **Actualizar ahora** comenzará el proceso de descarga y se mostrará el progreso del proceso de actualización. Para interrumpir la actualización, haga clic en **Cancelar actualización**.

IMPORTANTE: en circunstancias normales, si las actualizaciones se descargan adecuadamente, se mostrará el mensaje **No es necesario realizar la actualización: la base de firmas de virus instalada está actualizada** en la ventana **Actualización**. En caso contrario, el programa no estará actualizado y es más vulnerable a la infección. Actualice la

base de firmas de virus tan pronto como sea posible. De lo contrario, se mostrará uno de los mensajes siguientes:

La base de firmas de virus está desactualizada: este error aparecerá tras varios intentos sin éxito de actualizar la base de firmas de virus. Le recomendamos que compruebe la configuración de actualización. La causa más frecuente de este error es la introducción incorrecta de los datos de autenticación o una mala configuración de la conexión.

La notificación anterior está relacionada con los dos mensajes **No se ha podido actualizar la base de firmas de virus** siguientes sobre actualizaciones incorrectas:

Licencia no válida: la clave de licencia se ha introducido en la configuración de actualización de forma incorrecta. Recomendamos que compruebe sus datos de autenticación. La ventana Configuración avanzada (pulse F5 en el teclado) contiene opciones de actualización adicionales. Haga clic en **Ayuda y soporte** > **Administrar licencia** en el menú principal para introducir una nueva clave de licencia.

Se produjo un error al descargar los archivos de actualización: el error puede deberse a una configuración de la conexión a Internet incorrecta. Es recomendable que compruebe la conectividad a Internet (por ejemplo, mediante la apertura de un sitio web en el navegador web). Si el sitio web no se abre, es probable que no se haya establecido ninguna conexión a Internet o que haya problemas de conectividad con el ordenador. Consulte a su proveedor de servicios de Internet (ISP) si no tiene una conexión activa a Internet.

NOTA: consulte este artículo de la base de conocimiento de ESET para obtener más información.

4.5.1 Configuración de la actualización de la base de firmas de virus

La actualización de la base de firmas de virus y de los componentes del programa es importante a la hora de proporcionar protección total frente a código malicioso. Preste especial atención a su configuración y funcionamiento. En el menú principal, seleccione **Actualización** y, a continuación, haga clic en **Actualizar ahora** para comprobar si hay alguna actualización de la base de firmas de virus más reciente.

Puede configurar los ajustes de actualización desde la ventana Configuración avanzada (pulse la tecla F5 del teclado). Para configurar las opciones avanzadas de actualización, como el modo de actualización, el acceso al servidor Proxy, la conexión de red local y la configuración de copia de la base de firmas de virus (mirror), haga clic en el botón **Actualización** de la ventana **Configuración avanzada** disponible a la izquierda. Si tiene problemas con la actualización, haga clic en el botón **Borrar caché** para vaciar la carpeta de actualización temporal. El menú **Servidor de actualización** está establecido en **AUTOSELECT** de forma predeterminada. **AUTOSELECT** significa que el servidor de actualizaciones del que se descargan las actualizaciones de la base de firmas de virus se elige automáticamente. Se recomienda mantener seleccionada la opción predeterminada. Si no desea que aparezca la notificación de la bandeja del sistema en la esquina inferior derecha de la pantalla, seleccione **Desactivar la notificación de la actualización correcta**.

Para optimizar la funcionalidad, es importante que el programa se actualice automáticamente. Esto solo es posible si se introduce la **clave de licencia** correcta en **Ayuda y asistencia técnica** > **Activar licencia.**

Si no activó su producto después de la instalación, puede hacerlo en cualquier momento. Para obtener más información detallada sobre la activación, consulte Cómo activar ESET Mail Security e introduzca los datos de licencia que recibió al adquirir el producto de seguridad de ESET en la ventana Detalles de la licencia.

4.5.2 Configuración del servidor proxy para las actualizaciones

Si utiliza un servidor proxy para la conexión a Internet en un sistema en el que está instalado ESET Mail Security, los ajustes del proxy deberán configurarse en la sección Configuración avanzada. Para acceder a la ventana de configuración del servidor proxy, pulse F5 para abrir la ventana Configuración avanzada y haga clic en **Actualización** > **Proxy HTTP**. Seleccione **Conexión a través de un servidor proxy** en el menú desplegable **Modo proxy** y especifique los detalles de su servidor proxy: **Servidor proxy** (dirección IP), número de **Puerto** y **Nombre de usuario** y **Contraseña** (si procede).

Si no está seguro de cuáles son los datos del servidor proxy, puede intentar detectar automáticamente la configuración del proxy mediante la selección de **Usar la configuración global del servidor proxy** en la lista desplegable.

NOTA: Las opciones del servidor Proxy pueden ser diferentes para los distintos perfiles de actualización. Si este es el caso, configure los distintos perfiles de actualización en la opción Configuración avanzada; para ello haga clic en **Actualización** > **Perfil**.

4.6 Configuración

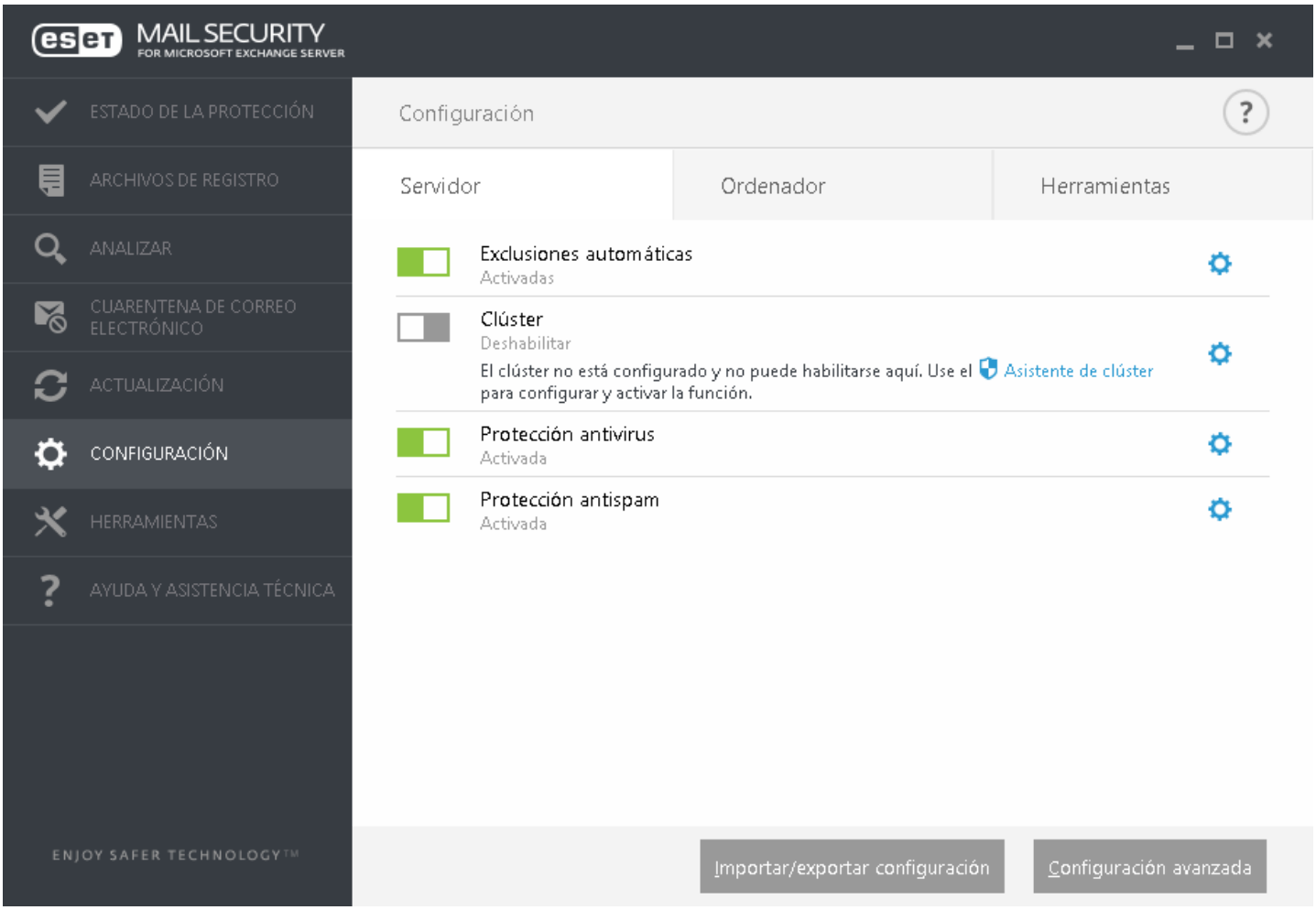
El menú Configuración consta de tres fichas:

- Servidor
- Ordenador
- Herramientas

4.6.1 Servidor

ESET Mail Security protege el servidor con funciones esenciales como las siguientes: Antivirus y antiespía, Protección residente (protección en tiempo real), Protección del tráfico de Internet y Protección del cliente de correo electrónico. Encontrará más información sobre los diferentes tipos de protección en ESET Mail Security: ordenador.

- Exclusiones automáticas: esta función identifica las aplicaciones de servidor y los archivos del sistema operativo fundamentales, y los añade a la lista de Exclusiones. Esta funcionalidad minimiza el riesgo de sufrir conflictos y aumenta el rendimiento general del servidor durante la ejecución de software antivirus.
- Para configurar el Clúster de ESET, haga clic en **Asistente de clúster**. Si desea obtener más información sobre cómo configurar el Clúster de ESET con la ayuda del asistente, haga clic aquí.
- **Antivirus protection** - guards against malicious system attacks by controlling file, email and Internet communication.
- **Antispam protection** - integrates several technologies (RBL, DNSBL, Fingerprinting, Reputation checking, Content analysis, Bayesian filtering, Rules, Manual whitelisting/blacklisting, etc.) to achieve maximum detection of email threats.



Si desea establecer opciones más detalladas, haga clic en **Configuración avanzada** o pulse **F5**.

En la parte inferior de la ventana de configuración encontrará opciones adicionales. Para cargar los parámetros de configuración con un archivo de configuración *.xml*, o para guardar los parámetros de configuración actuales en un archivo de configuración, utilice la opción **Importar/exportar configuración**. Consulte Importar/exportar configuración para obtener más información detallada.

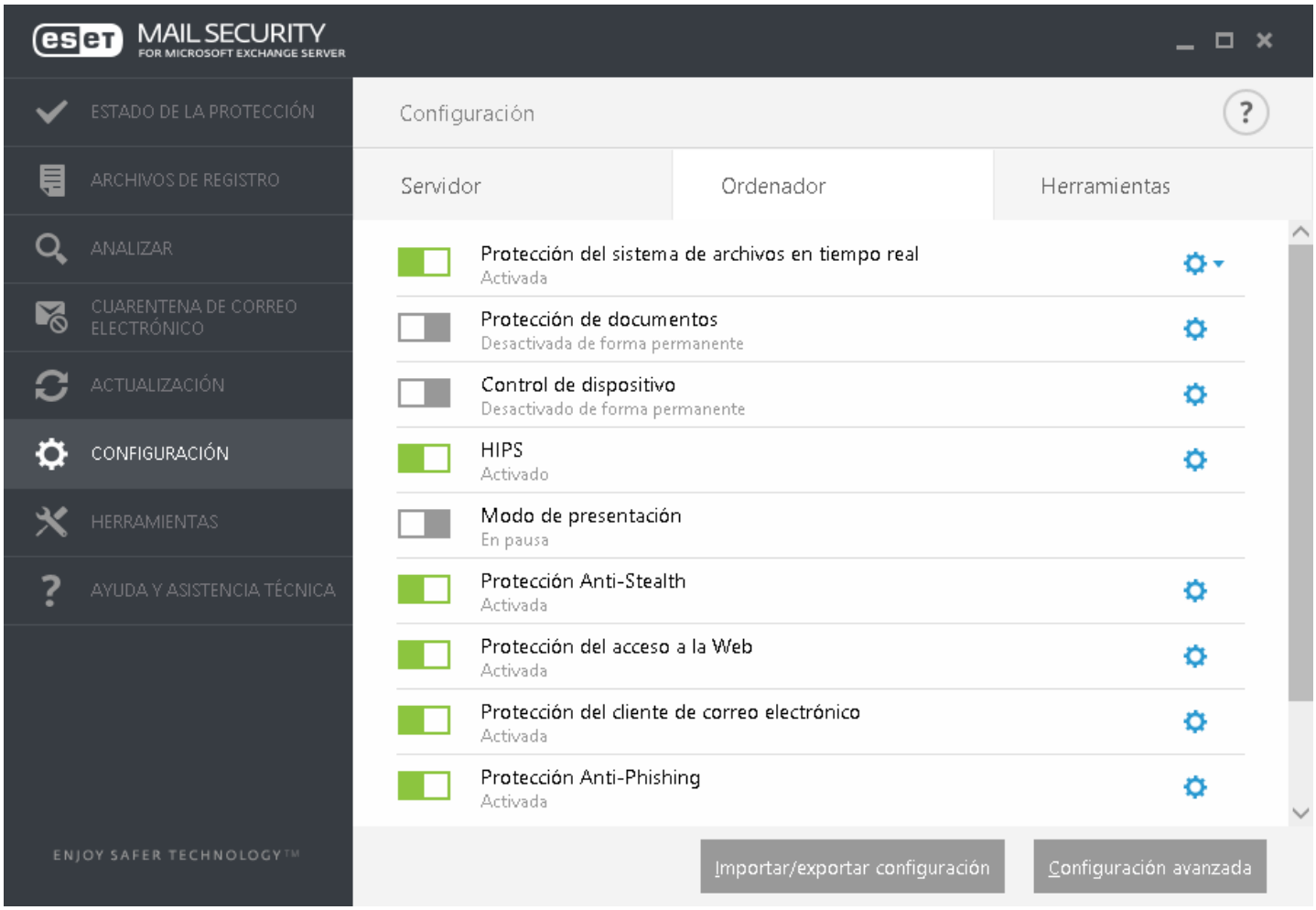
4.6.2 Ordenador

ESET Mail Security incluye todos los componentes necesarios para garantizar una protección eficaz del servidor como ordenador. Cada uno de los componentes presta un tipo de protección concreto, como: Antivirus y antiespía, Protección del sistema de archivos en tiempo real, Protección del tráfico de Internet, Cliente de correo electrónico, Protección Anti-Phishing, etc.

La sección **Ordenador** se encuentra en **Configuración** > **Ordenador**. Verá una lista de componentes que puede activar y desactivar con el conmutador . Si desea configurar los ajustes de un elemento concreto, haga clic en la rueda dentada . En el caso de la **Protección del sistema de archivos en tiempo real** existe también la opción de **Editar exclusiones**, con lo que se abrirá la ventana de configuración de Exclusiones, en la que puede excluir archivos y carpetas del análisis.

Pausar la protección antivirus y antiespía: cuando desactive la protección antivirus y antiespía de forma temporal, utilice el menú desplegable para seleccionar el período de tiempo durante el que desea que el componente seleccionado esté desactivado y, a continuación, haga clic en **Aplicar** para desactivar el componente de seguridad. Para volver a activar la protección, haga clic en **Activar la protección antivirus y antiespía**.

El módulo **Ordenador** le permite activar/desactivar y configurar los siguientes componentes:



- **Protección del sistema de archivos en tiempo real**: todos los archivos se analizan en busca de código malicioso en el momento de abrirlos, crearlos o ejecutarlos en el ordenador.
- **Protección de documentos**: la función de protección de documentos analiza los documentos de Microsoft Office antes de que se abran, además de los archivos descargados automáticamente con Internet Explorer, como los elementos de Microsoft ActiveX.
- **Control de dispositivos**: este módulo le permite analizar, bloquear o ajustar los filtros y permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo dado y trabajar en él.
- **HIPS**: el sistema HIPS controla los sucesos del sistema operativo y reacciona según un conjunto de reglas personalizado.
- **Modo de presentación**: es una función pensada para aquellos usuarios que exigen un uso del software sin interrupciones y sin ventanas emergentes, así como un menor uso de la CPU. Cuando se active el Modo de presentación recibirá un mensaje de alerta (posible riesgo de seguridad) y la ventana principal del programa cambiará a color naranja.
- **Protección Anti-Stealth**: detecta programas peligrosos (como los rootkits) que pueden ocultarse del sistema operativo. Esto implica que no es posible detectarlos mediante las técnicas habituales.
- **Protección del tráfico de Internet**: si esta opción está activada, se analiza todo el tráfico a través de HTTP o HTTPS para detectar la presencia de software malicioso.
- **Protección del cliente de correo electrónico**: controla las comunicaciones recibidas a través de los protocolos POP3 e IMAP.
- **Protección Anti-Phishing**: le protege de intentos de adquirir contraseñas, datos bancarios y otra información confidencial por parte de sitios web que suplantan a sitios legítimos.

NOTA: la opción Protección de documentos está desactivada de forma predeterminada. Si desea activarla, haga clic en el icono del conmutador.

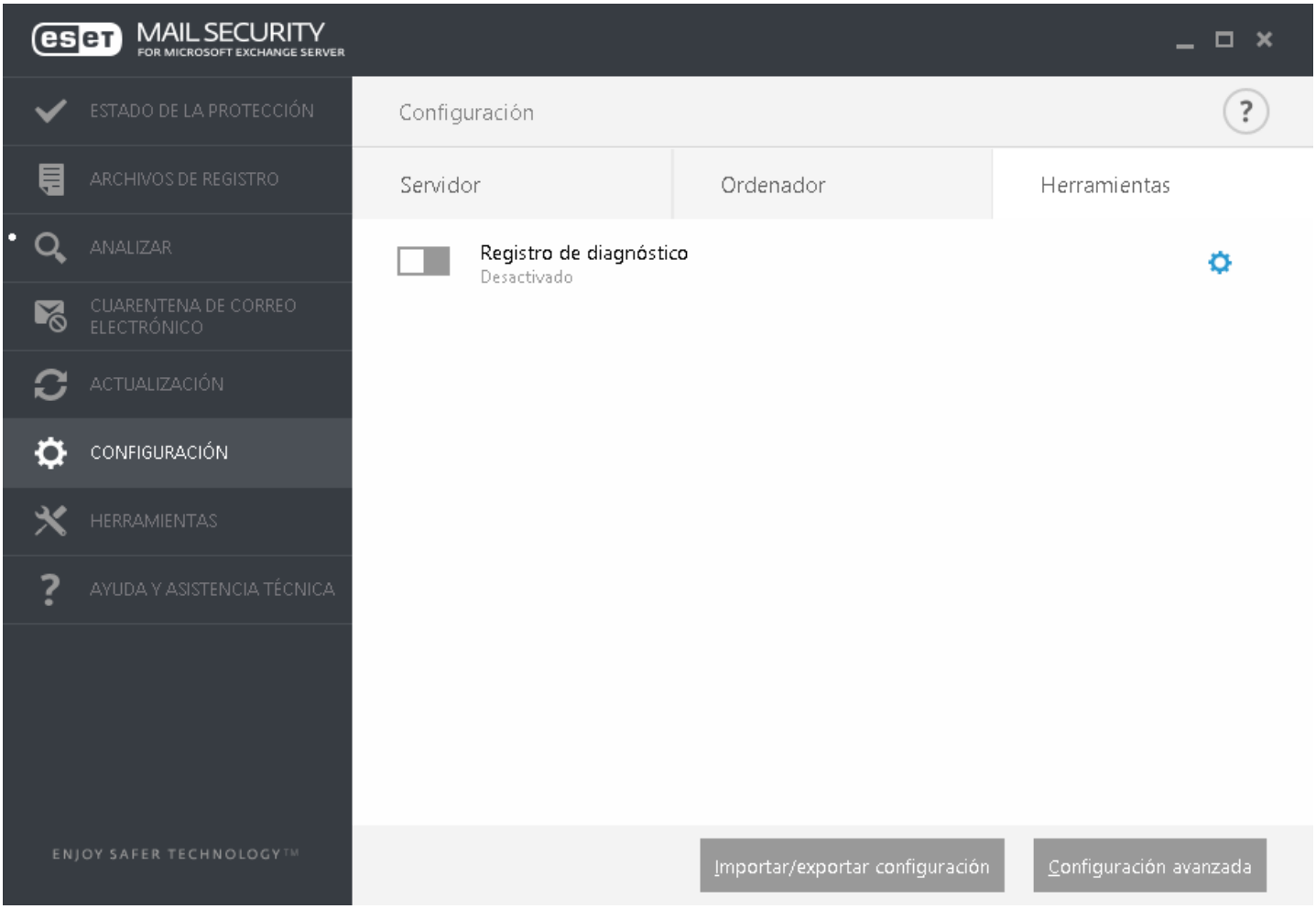
En la parte inferior de la ventana de configuración encontrará opciones adicionales. Para cargar los parámetros de configuración con un archivo de configuración *.xml*, o para guardar los parámetros de configuración actuales en un

archivo de configuración, utilice la opción **Importar/exportar configuración**. Consulte Importar/exportar configuración para obtener más información detallada.

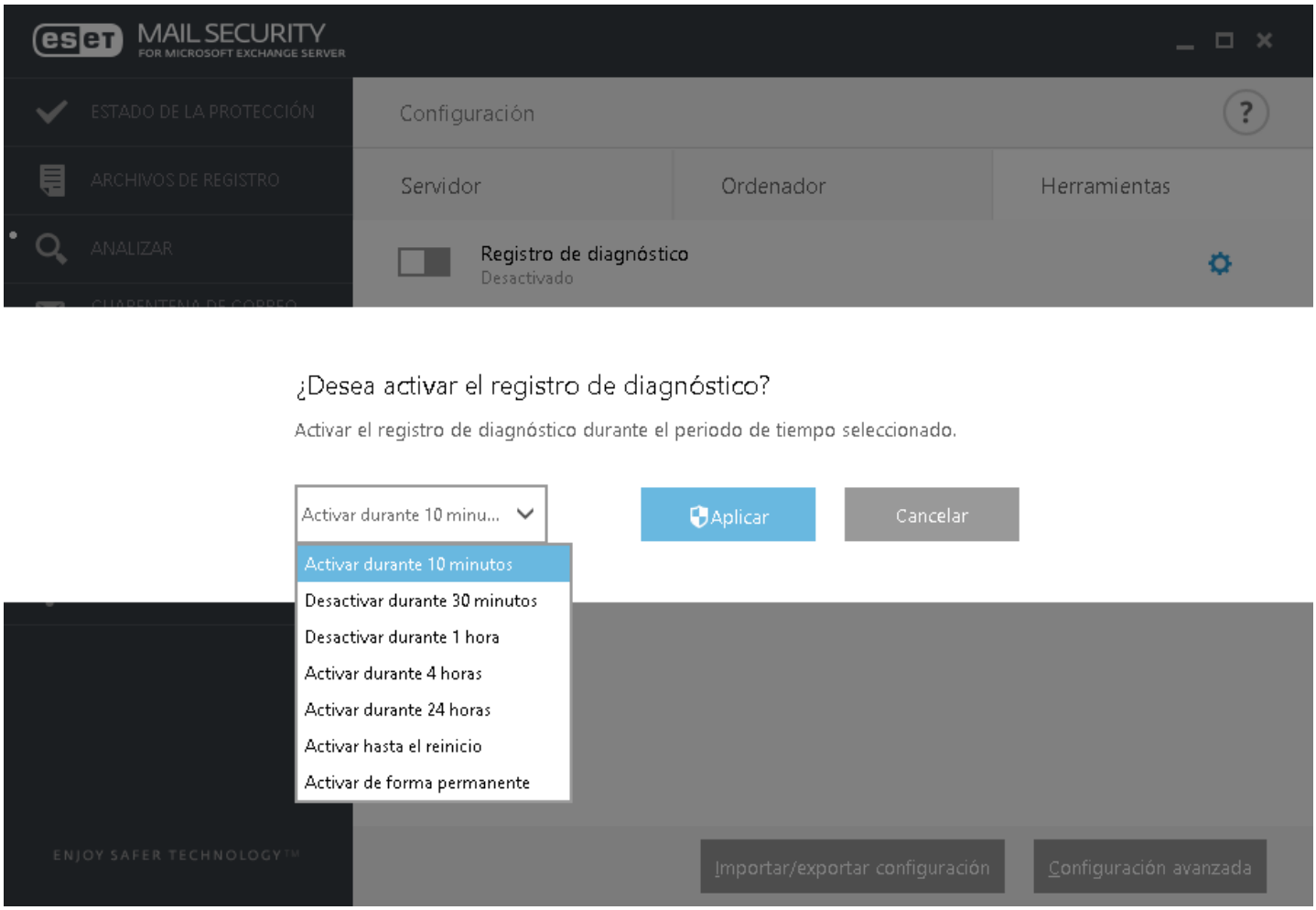
Si desea establecer opciones más detalladas, haga clic en **Configuración avanzada** o pulse **F5**.

4.6.3 Herramientas

Registro de diagnóstico: configure qué componentes escribirán registros de diagnóstico cuando el registro de diagnóstico esté activado. Al hacer clic en el conmutador para activar el registro de diagnóstico, puede elegir cuánto tiempo estará activado (10 minutos, 30 minutos, 1 hora, 4 horas, 24 horas, hasta el siguiente reinicio del servidor o permanentemente). Los componentes que no aparecen en esta ficha escriben siempre registros de diagnóstico.



- **Activar** el registro de diagnóstico durante el periodo de tiempo seleccionado.



4.6.4 Importar y exportar configuración

Las opciones de importación y exportación de la configuración de ESET Mail Security están disponibles en **Configuración** al hacer clic en **Importar/Exportar configuración**.

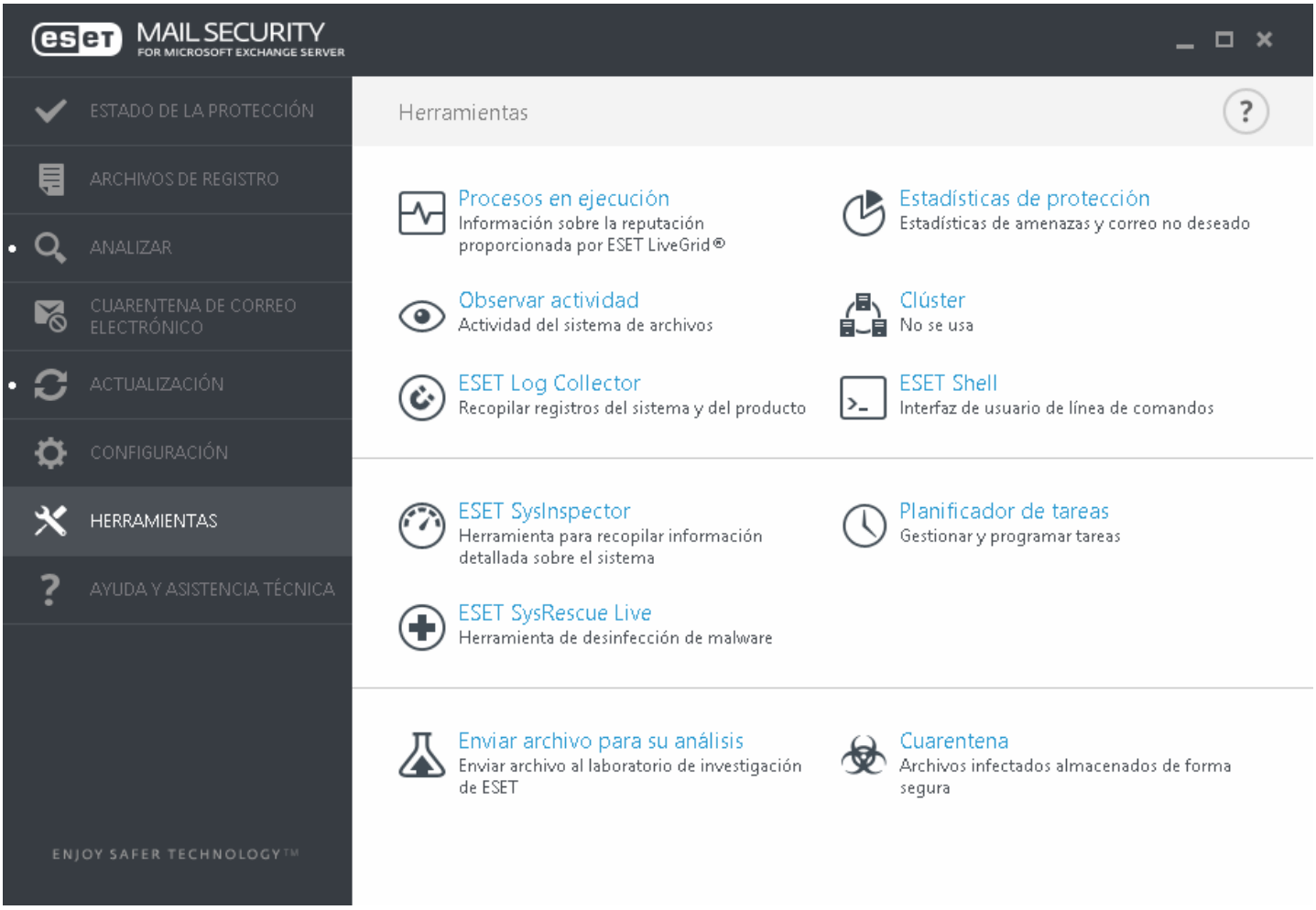
Tanto en la importación como en la exportación se utiliza el tipo de archivo .xml. Las opciones de importación y exportación resultan útiles en aquellos casos en los que necesita realizar una copia de seguridad de la configuración actual de ESET Mail Security. Esta puede usarse posteriormente para aplicar la misma configuración a otros ordenadores.

Importar y exportar configuración
La configuración actual de ESET Mail Security se puede guardar en un archivo XML para restaurarla posteriormente cuando sea necesaria.
Importar y exportar
Importar configuración
Exportar configuración
Ruta del archivo:
...
Aceptar
Cancelar

4.7 Herramientas

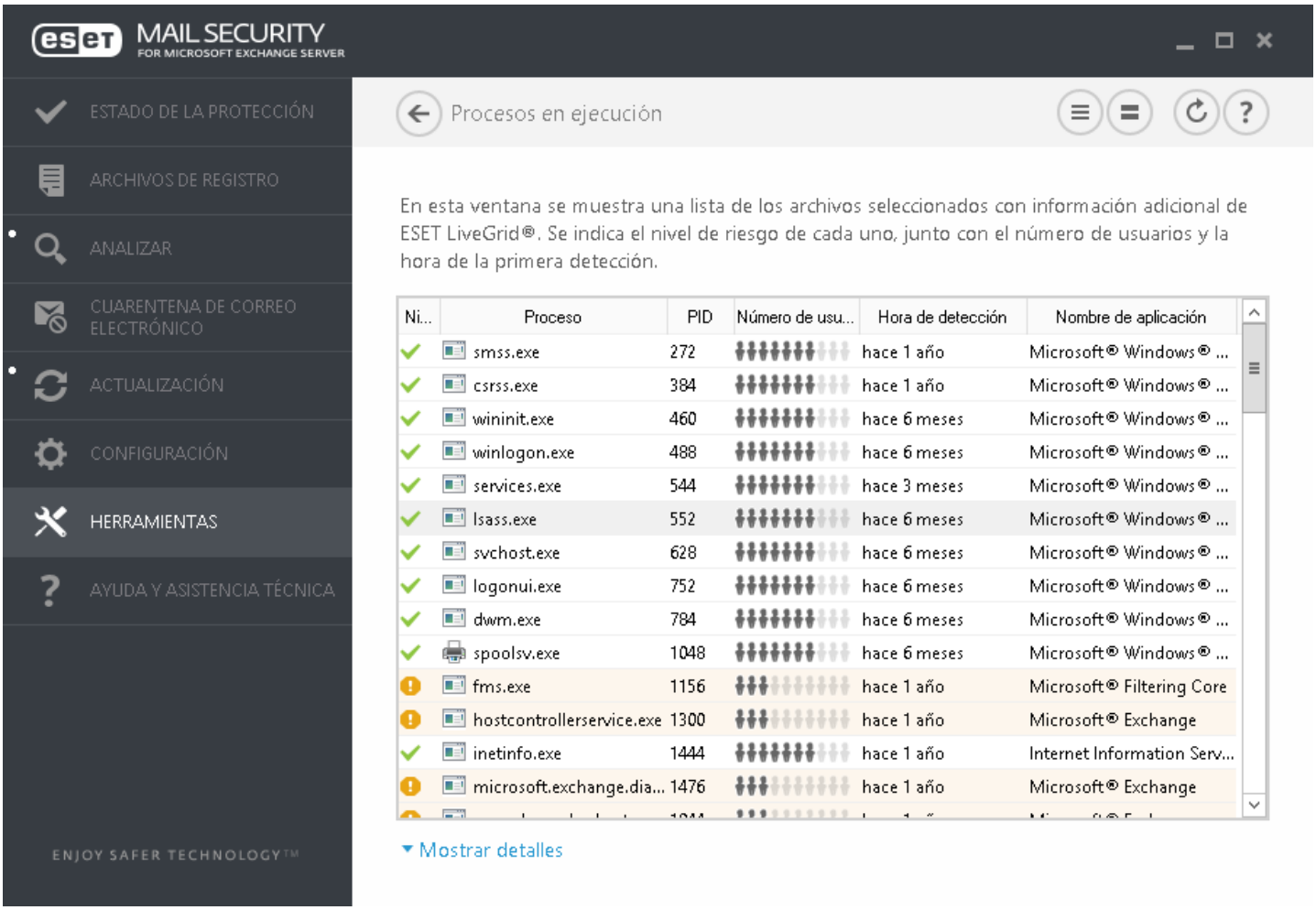
El menú Herramientas incluye módulos que ayudan a simplificar la administración del programa y ofrecen opciones adicionales. En él podemos encontrar las siguientes herramientas:

- Procesos en ejecución
- Observar actividad
- ESET Log Collector
- Estadísticas de protección
- Clúster
- ESET Shell
- ESET SysInspector
- ESET SysRescue Live
- Planificador de tareas
- Enviar muestra para el análisis
- Cuarentena



4.7.1 Procesos en ejecución

En Procesos en ejecución se indican los programas o procesos que se están ejecutando en el ordenador y se informa a ESET de forma inmediata y continua de las nuevas amenazas. ESET Mail Security proporciona información detallada sobre los procesos en ejecución para proteger a los usuarios con la tecnología ESET Live Grid activada.


MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
ESTADO DE LA PROTECCIÓN
ARCHIVOS DE REGISTRO
ANALIZAR
CUARENTENA DE CORREO ELECTRÓNICO
ACTUALIZACIÓN
CONFIGURACIÓN
HERRAMIENTAS
AYUDA Y ASISTENCIA TÉCNICA
ENJOY SAFER TECHNOLOGY™
Procesos en ejecución
En esta ventana se muestra una lista de los archivos seleccionados con información adicional de ESET LiveGrid®. Se indica el nivel de riesgo de cada uno, junto con el número de usuarios y la hora de la primera detección.
Ni... Proceso PID Número de usu... Hora de detección Nombre de aplicación
smss.exe 272 hace 1 año Microsoft® Windows® ...
csrss.exe 384 hace 1 año Microsoft® Windows® ...
wininit.exe 460 hace 6 meses Microsoft® Windows® ...
winlogon.exe 488 hace 6 meses Microsoft® Windows® ...
services.exe 544 hace 3 meses Microsoft® Windows® ...
lsass.exe 552 hace 6 meses Microsoft® Windows® ...
svchost.exe 628 hace 6 meses Microsoft® Windows® ...
logonui.exe 752 hace 6 meses Microsoft® Windows® ...
dwm.exe 784 hace 6 meses Microsoft® Windows® ...
spoolsv.exe 1048 hace 6 meses Microsoft® Windows® ...
fms.exe 1156 hace 1 año Microsoft® Filtering Core
hostcontrollerservice.exe 1300 hace 1 año Microsoft® Exchange
inetinfo.exe 1444 hace 1 año Internet Information Serv...
microsoft.exchange.dia... 1476 hace 1 año Microsoft® Exchange
Mostrar detalles

Nivel de riesgo: generalmente, ESET Mail Security y la tecnología ESET Live Grid asignan un nivel de riesgo a los objetos (archivos, procesos, claves de registro, etc.). Para ello, utilizan una serie de reglas heurísticas que examinan las características de cada objeto y, después, pondera el potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asignará un nivel de riesgo desde el valor "1: correcto" (verde) hasta "9: peligroso" (rojo).

Proceso: nombre de la imagen del programa o proceso que se está ejecutando en el ordenador. También puede utilizar el Administrador de tareas de Windows para ver todos los procesos que están en ejecución en el ordenador. Para abrir el Administrador de tareas, haga clic con el botón derecho del ratón en un área vacía de la barra de tareas y, a continuación, haga clic en Administrador de tareas o pulse la combinación **Ctrl** + **Mayús** + **Esc** en el teclado.

PID: se trata de un identificador de los procesos que se ejecutan en sistemas operativos Windows.

NOTA: las aplicaciones conocidas marcadas como Correcto (verde) son totalmente seguras (incluidas en lista blanca) y no se analizan; esto aumenta la velocidad del análisis a petición del ordenador o la protección del sistema de archivos en tiempo real.

Número de usuarios: el número de usuarios que utilizan una aplicación determinada. La tecnología ESET Live Grid se encarga de recopilar esta información.

Tiempo de detección: tiempo transcurrido desde que la tecnología ESET Live Grid detectó la aplicación.

NOTA: cuando una aplicación está marcada con el nivel de seguridad Desconocido (naranja), no siempre se trata de software malicioso. Normalmente, se trata de una aplicación reciente. Si el archivo le plantea dudas, utilice la característica Enviar muestra para su análisis para enviarlo al laboratorio de virus de ESET. Si resulta que el archivo es una aplicación maliciosa, su detección se agregará a una de las siguientes actualizaciones de la base de firmas de

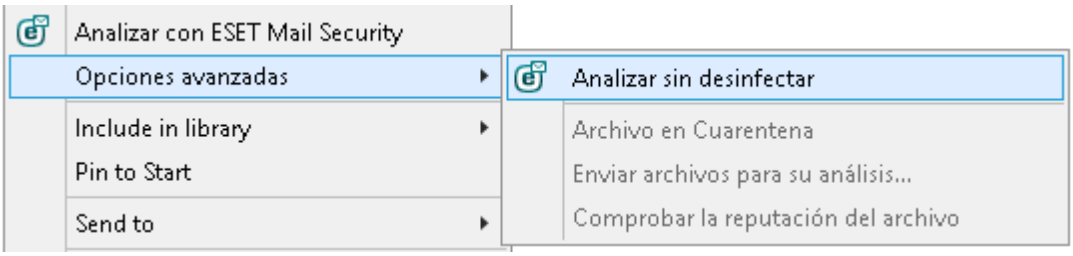
virus.

Nombre de aplicación: nombre del programa al que pertenece este proceso.

Al hacer clic en una aplicación en la parte inferior se mostrará la siguiente información en la parte inferior de la ventana:

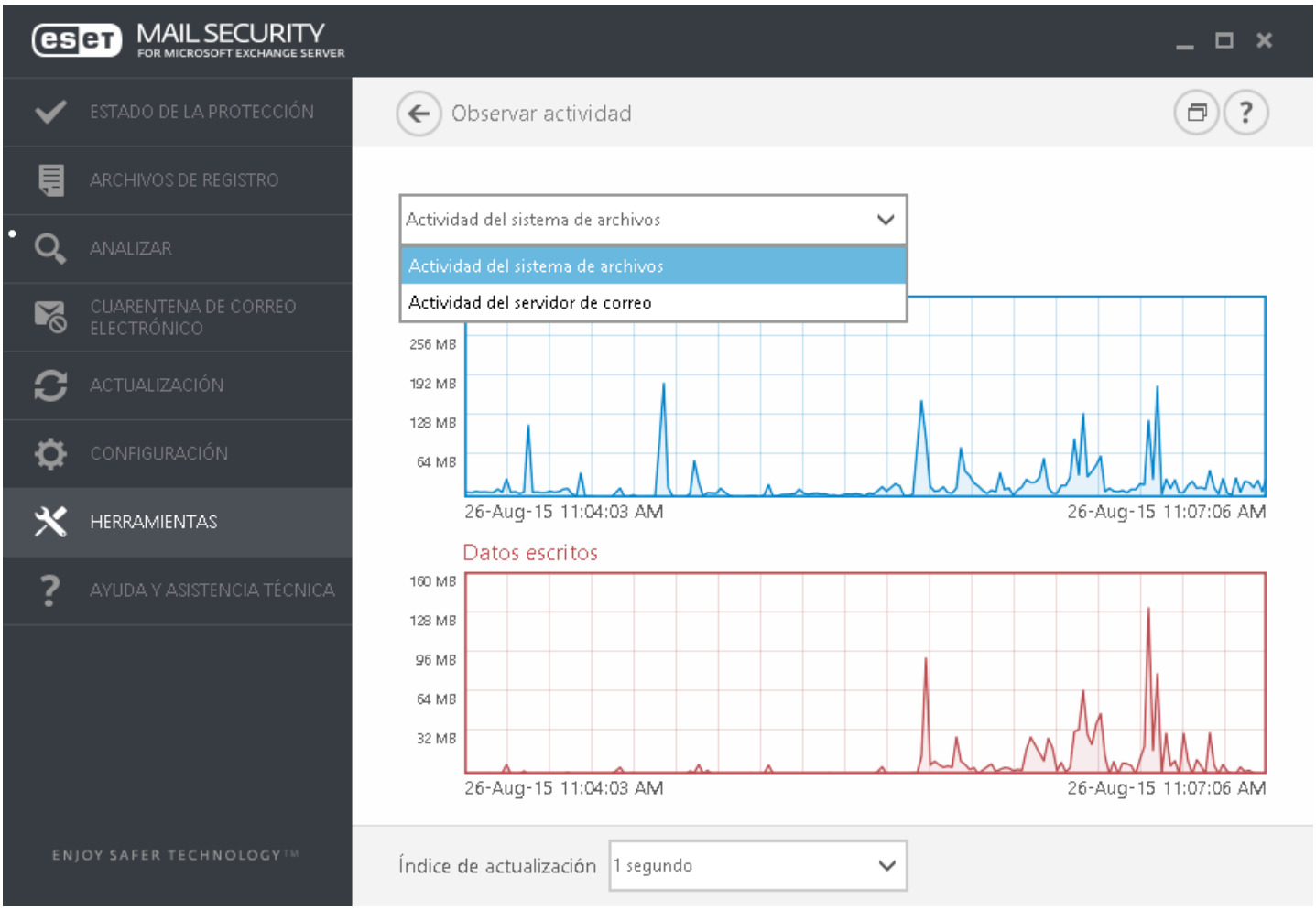
- **Ruta**: ubicación de una aplicación en el ordenador.
- **Tamaño**: tamaño del archivo en KB (kilobytes) o MB (megabytes).
- **Descripción**: características del archivo de acuerdo con la descripción del sistema operativo.
- **Empresa**: nombre del proveedor o el proceso de la aplicación.
- **Versión**: información sobre el editor de la aplicación.
- **Producto**: nombre de la aplicación o nombre comercial.
- **Fecha de creación**: fecha y hora en que se creó una aplicación.
- **Fecha de modificación**: última fecha y hora en que se modificó una aplicación.

NOTA: la reputación también se puede comprobar en los archivos que no actúan como programas o procesos en ejecución. - Para ejecutar dicha comprobación, seleccione los archivos que desea comprobar, haga clic con el botón derecho del ratón en ellos y, en el menú contextual, seleccione **Opciones avanzadas** > **Comprobar la reputación del archivo con ESET Live Grid**.



4.7.2 Observar actividad

Para ver la **Actividad del sistema de archivos** actual y la **Actividad del servidor de correo** en formato gráfico, haga clic en **Herramientas** > **Observar actividad**. Muestra dos gráficos con la cantidad de datos leídos y escritos en el sistema. En la parte inferior del gráfico hay una línea cronológica que registra la actividad del sistema de archivos en tiempo real en el intervalo de tiempo seleccionado. Si desea cambiar el intervalo de tiempo, realice la selección en el menú desplegable **Índice de actualización**.



Están disponibles las opciones siguientes:

- **1 segundo**: el gráfico se actualiza cada segundo y la línea cronológica abarca los últimos 10 minutos.
- **1 minuto (últimas 24 horas)**: el gráfico se actualiza cada minuto y la línea cronológica abarca las últimas 24 horas.
- **1 hora (último mes)**: el gráfico se actualiza cada hora y la línea cronológica abarca el último mes.
- **1 hora (mes seleccionado)**: el gráfico se actualiza cada hora y la línea cronológica abarca el mes seleccionado. Haga clic en el botón **Cambiar mes** para efectuar otra selección.

El eje vertical del **Gráfico de actividad del sistema de** archivos representa la cantidad de datos leídos (azul) y escritos (rojo). Ambos valores se ofrecen en KB (kilobytes), MB o GB. Si pasa el ratón por encima de los datos leídos o escritos en la leyenda disponible debajo del gráfico, el gráfico solo mostrará datos de ese tipo de actividad.

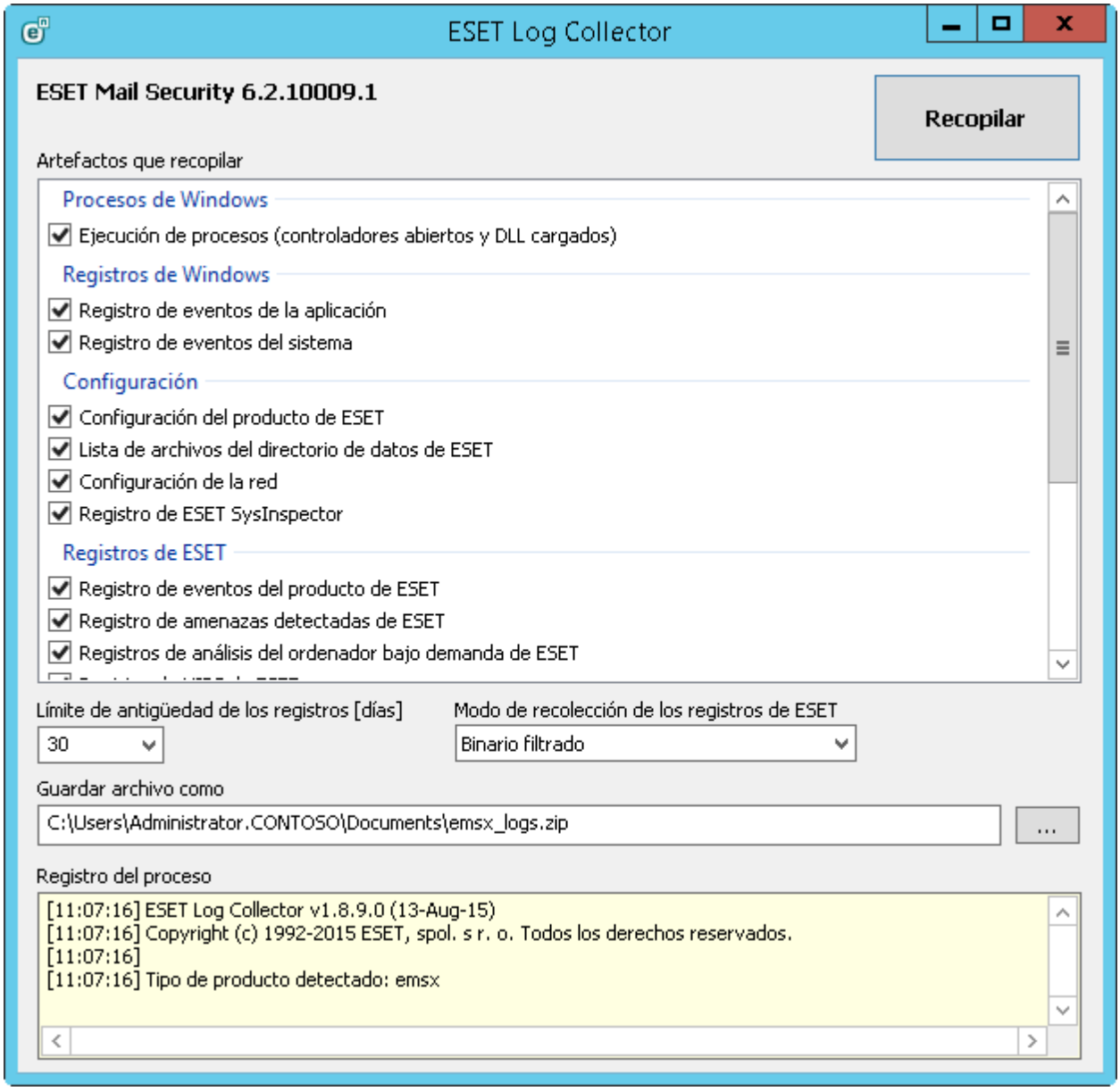
4.7.2.1 Selección del período de tiempo

Seleccione el mes (y el año) del que desea ver la **Actividad del sistema de archivos** o la **Actividad del servidor de correo** en el gráfico.

4.7.3 ESET Log Collector

ESET Log Collector es una aplicación que recopila automáticamente información (por ejemplo de configuración) y registros del servidor para contribuir a acelerar la resolución de problemas. Cuando tenga un caso abierto con el servicio de atención al cliente de ESET, podría pedírsele que facilitara registros de su ordenador. El Recolector de registros de ESET facilitará la recopilación de los datos necesarios.

Se puede acceder al menú principal de ESET Log Collector haciendo clic en **Herramientas** > **Recolector de registros de ESET**.


ESET Log Collector
ESET Mail Security 6.2.10009.1
Recopilar
Artefactos que recopilar
Procesos de Windows
Ejecución de procesos (controladores abiertos y DLL cargados)
Registros de Windows
Registro de eventos de la aplicación
Registro de eventos del sistema
Configuración
Configuración del producto de ESET
Lista de archivos del directorio de datos de ESET
Configuración de la red
Registro de ESET SysInspector
Registros de ESET
Registro de eventos del producto de ESET
Registro de amenazas detectadas de ESET
Registros de análisis del ordenador bajo demanda de ESET
Límite de antigüedad de los registros [días]
30
Modo de recolección de los registros de ESET
Binario filtrado
Guardar archivo como
C:\Users\Administrator.CONTOSO\Documents\emsx_logs.zip
...
Registro del proceso
[11:07:16] ESET Log Collector v1.8.9.0 (13-Aug-15)
[11:07:16] Copyright (c) 1992-2015 ESET, spol. s r. o. Todos los derechos reservados.
[11:07:16]
[11:07:16] Tipo de producto detectado: emsx

Active las casillas de verificación correspondientes a los registros que desee recopilar. Si no está seguro de qué elementos debe seleccionar, mantenga todas las casillas de verificación activadas (esta es la opción predeterminada). Especifique la ubicación en la que desea guardar los documentos del archivo y, a continuación, haga clic en **Guardar**. El nombre del archivo aparece ya predefinido. Haga clic en **Recopilar**.

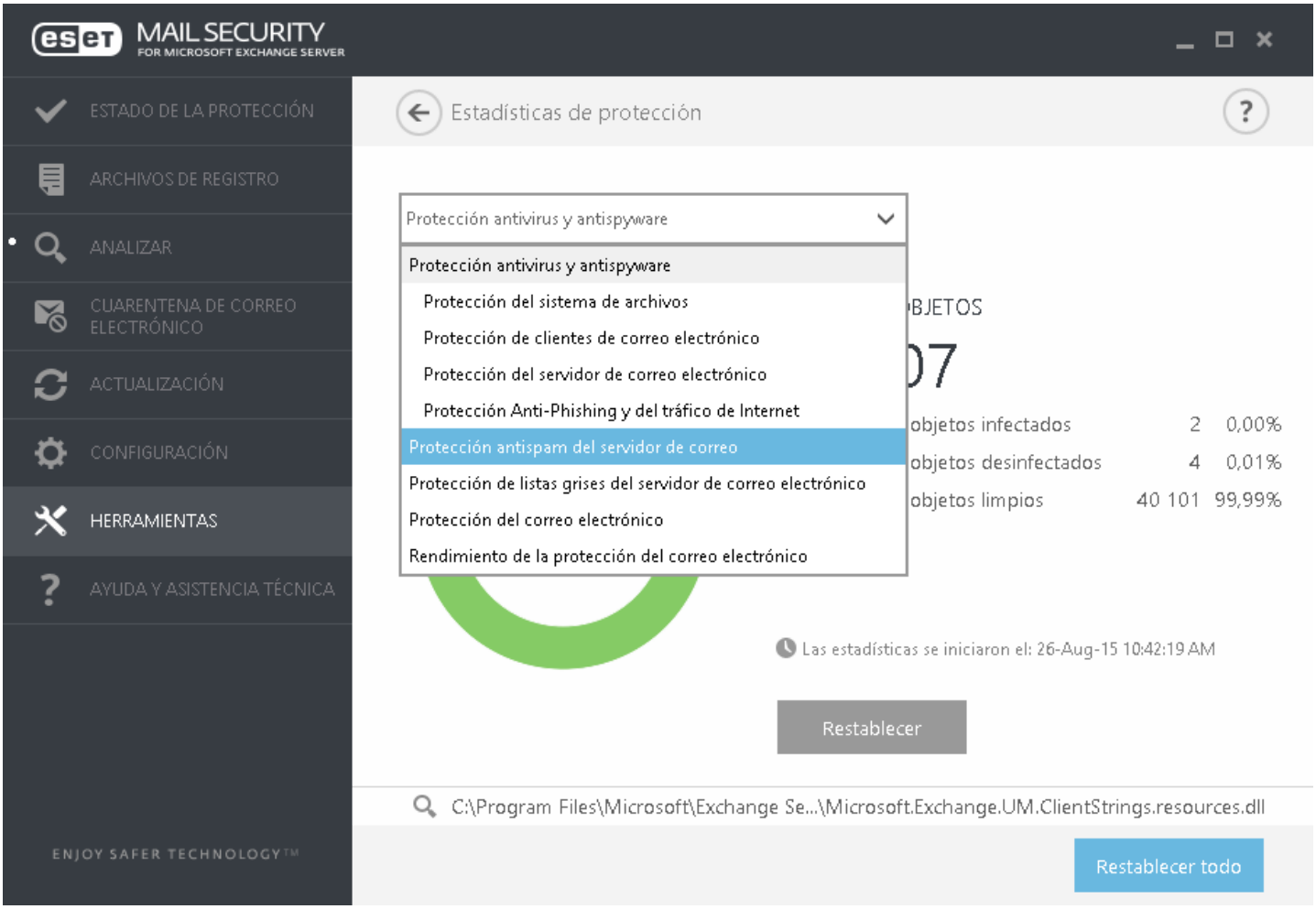
Durante el proceso de recopilación puede ver la ventana del registro de operaciones en la parte inferior de la pantalla, para así saber la operación que se está realizando actualmente. Una vez finalizado el proceso de recopilación se mostrarán todos los documentos que se hayan recopilado y archivado. Esto indica que el proceso de recopilación ha finalizado correctamente, y que el archivo (por ejemplo, `registros_emsx.zip`) se ha guardado en la

ubicación especificada.

Si desea obtener información sobre ESET Log Collector y sobre la lista de archivos que ESET Log Collector recopila, visite la base de conocimiento de ESET.

4.7.4 Estadísticas de protección

Para ver un gráfico de datos estadísticos sobre los módulos de protección de ESET Mail Security, haga clic en **Herramientas** > **Estadísticas de protección**. Seleccione el módulo de protección deseado en el menú desplegable para ver el gráfico y la leyenda correspondientes. Coloque el cursor del ratón sobre un elemento de la leyenda para mostrar en el gráfico los datos correspondientes a ese elemento.



Están disponibles los siguientes gráficos de estadísticas:

- **Protección antivirus y antiespía**: muestra el número total de objetos infectados y desinfectados.
- **Protección del sistema de archivos**: solo muestra objetos que se leyeron o escribieron en el sistema de archivos.
- **Protección del cliente de correo electrónico**: solo muestra objetos que se enviaron o recibieron a través de clientes de correo electrónico.
- **Protección del servidor de correo electrónico**: muestra los datos estadísticos de antivirus y antiespía del servidor de correo.
- **Protección del acceso a la Web y Anti-Phishing**: solo muestra objetos descargados por los navegadores web.
- **Protección antispam del servidor de correo**: muestra el historial de estadísticas de correo no deseado desde el último inicio.
- **Protección de listas grises del servidor de correo electrónico**: incluye estadísticas de correo no deseado generadas por el método de creación de listas grises.
- **Protección de la actividad de transporte de correo electrónico**: muestra los objetos comprobados, bloqueados y eliminados por el servidor de correo.
- **Rendimiento de la protección del transporte del correo electrónico**: muestra los datos procesados por el agente de transporte/VSAPI en B/s.
- **Protección de la actividad de la base de datos de buzones**: muestra los objetos procesados por VSAPI (número de objetos **verificados**, **puestos en cuarentena** y **eliminados**).
- **Rendimiento de la protección de la base de datos de buzones**: muestra los datos procesados por VSAPI (número de medias diferentes durante **Hoy**, durante los **Últimos 7 días** y medias **Desde el último restablecimiento**).

Junto a los gráficos de estadísticas puede ver el número de todos los objetos analizados, infectados, desinfectados y sin infecciones. Haga clic **Restablecer** para borrar los datos estadísticos o haga clic en **Restablecer todo** para borrar y eliminar todos los datos disponibles.

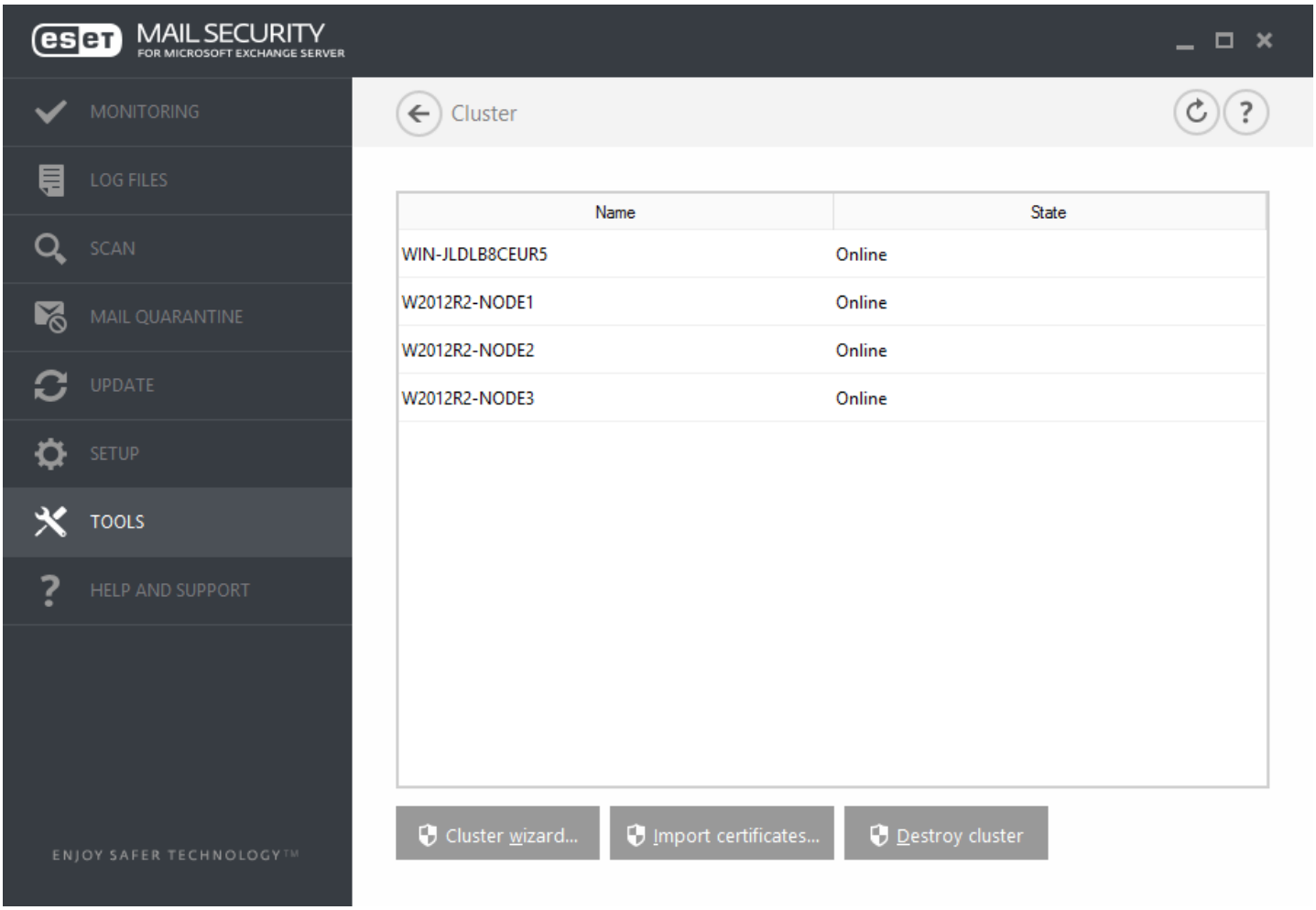
4.7.5 Clúster

El **Clúster de ESET** es una infraestructura de comunicación P2P de la gama de productos ESET para Microsoft Windows Server.

Esta infraestructura permite que los productos de servidor de ESET se comuniquen e intercambien datos como, por ejemplo, configuraciones y notificaciones, además de sincronizar los datos necesarios para el correcto funcionamiento de un grupo de instancias del producto. Un ejemplo de este tipo de grupo es un grupo de nodos de un clúster de conmutación por error de Windows o un clúster de equilibrio de carga de red (NLB) con un producto ESET instalado en el que es necesario que el producto tenga la misma configuración en todo el clúster. Clúster de ESET garantiza esta coherencia entre instancias.

NOTA: los ajustes de la interfaz de usuario no se sincronizan entre los nodos del Clúster de ESET.

A la página de estado de Clúster de ESET se accede desde el menú principal, con la ruta **Herramientas** > **Clúster**; cuando está correctamente configurado, la apariencia de la página de estado debe ser la siguiente:



Para configurar el Clúster de ESET, haga clic en **Asistente de clúster...** Si desea obtener más información sobre cómo configurar el Clúster de ESET con la ayuda del asistente, haga clic aquí.

Durante la configuración del Clúster de ESET hay dos formas de agregar los nodos: una automática, usando el clúster de conmutación por error o el clúster NLB actual, o examinando manualmente los ordenadores que se encuentran en un grupo de trabajo o en un dominio.

Detección automática: detecta automáticamente aquellos nodos que ya son miembros de un clúster de conmutación por error de Windows o NLB y los agrega al Clúster de ESET.
Examinar: permite agregar los nodos manualmente escribiendo el nombre de los servidores (tanto miembros del mismo grupo de trabajo como miembros del mismo dominio).

NOTA: no es necesario que los servidores sean miembros de un clúster de conmutación por error de Windows o de un clúster NLB para poder usar la función Clúster de ESET. No es necesario que haya un clúster de conmutación por error de Windows ni un clúster NLB en el entorno para poder usar los clústeres de ESET.

Tras agregar los nodos a su Clúster de ESET, el siguiente paso del proceso es instalar ESET Mail Security en cada nodo. Esta tarea se realiza automáticamente durante la configuración del Clúster de ESET.

Credenciales necesarias para la instalación remota de ESET Mail Security en otros nodos del clúster:

- Entorno de dominio: credenciales de administrador del dominio.
- Entorno de grupo de trabajo: debe asegurarse de que todos los nodos usan las credenciales de la misma cuenta de administrador local.

En un Clúster de ESET también puede usar una combinación de nodos agregados automáticamente como miembros de un clúster de conmutación por error de Windows o NLB y nodos agregados manualmente (siempre que estén en el mismo dominio).

NOTA: no es posible combinar nodos de dominio con nodos de grupo de trabajo.

Otro de los requisitos de uso del Clúster de ESET es que debe estar activada la opción **Compartir archivos e impresoras** en el Firewall de Windows antes de insertar la instalación de ESET Mail Security en los nodos de Clúster de ESET.

En caso de ser necesario, el Clúster de ESET puede desmantelarse fácilmente haciendo clic en **Destruir clúster**. Cada uno de los nodos anotará una entrada en su registro de sucesos en relación a la destrucción del Clúster de ESET. A continuación, todas las reglas del cortafuegos de ESET se eliminan del Firewall de Windows. Los antiguos nodos recuperarán su estado anterior, y pueden usarse de nuevo en otro Clúster de ESET, si así se desea.

NOTA: no es posible crear un Clúster de ESET entre ESET Mail Security y ESET File Security para Linux.

Es posible agregar nodos nuevos a un Clúster de ESET existente en cualquier momento ejecutando el **Asistente de clúster** como se ha explicado anteriormente y aquí.

4.7.6 ESET Shell

eShell (abreviación de ESET Shell) es una interfaz de línea de comandos para ESET Mail Security. Se trata de una alternativa a la interfaz gráfica de usuario (GUI). eShell tiene todas las características y opciones que suele ofrecer una interfaz gráfica de usuario; además, le permite configurar y administrar todo el programa sin necesidad de utilizar la GUI.

Además de todas las funciones y características disponibles en la GUI, también le ofrece una función de automatización mediante la ejecución de scripts para configurar, modificar una configuración o realizar una acción. eShell también puede ser de utilidad para aquellos que prefieren utilizar la línea de comandos en vez de la GUI.

eShell se puede ejecutar en dos modos:

- Modo interactivo: es útil para trabajar con eShell (no simplemente ejecutar un comando); por ejemplo, para realizar tareas como cambiar la configuración o ver los registros. También puede utilizar el modo interactivo si aún no está familiarizado con todos los comandos, ya que facilita la navegación por eShell. En este modo, se muestran los comandos disponibles para un contexto determinado.
- Modo por lotes/un solo comando: utilice este modo sin tan solo necesita ejecutar un comando, sin acceder al modo interactivo de eShell. Puede hacer esto desde la ventana de símbolo del sistema de Windows, escribiendo `eshell` y los parámetros adecuados. Por ejemplo:

```
eshell get status
```

o

```
eshell set antivirus status disabled
```

Para poder ejecutar determinados comandos (como el del segundo ejemplo anterior) en el modo por lotes/de script, debe configurar primero algunos ajustes. De lo contrario, se mostrará el mensaje **Acceso denegado**. Esto se debe a cuestiones de seguridad.

NOTA: recomendamos que, para esta función, abra eShell con la opción **Ejecutar como administrador**. La misma recomendación se aplica a la ejecución de un solo comando desde el símbolo del sistema de Windows (cmd). Abra el cmd con **Ejecutar como administrador**. De lo contrario, no podrá ejecutar todos los comandos. Esto se debe a que cuando abre cmd o eShell con una cuenta que no sea de administrador no dispone de permisos suficientes.

NOTA: para ejecutar comandos de eShell desde la ventana de símbolo del sistema de Windows o ejecutar archivos por lotes, primero debe realizar algunos ajustes. Si desea obtener más información sobre la ejecución de archivos por lotes, haga clic aquí.

Puede acceder al modo interactivo de eShell con estos dos métodos:

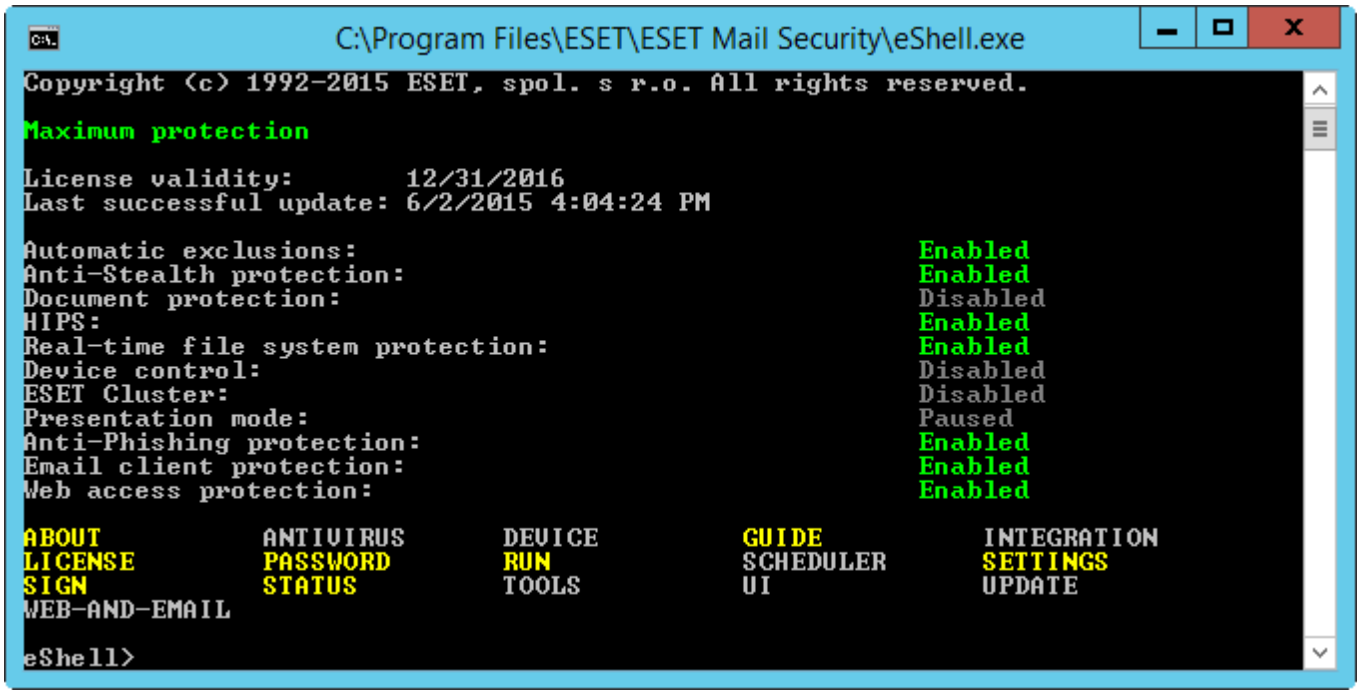
- Desde el menú Inicio de Windows: **Inicio** > **Todos los programas** > **ESET** > **ESET Mail Security** > **ESET shell**
- Desde la ventana de símbolo del sistema de Windows, escribiendo `eshell` y pulsando la tecla Intro.

La primera vez que ejecute eShell en modo interactivo, se mostrará la pantalla de primera ejecución (una guía).

NOTA: si desea ver otra vez la pantalla de primera ejecución, introduzca el comando `guide` . En esta pantalla se muestran varios ejemplos sencillos de cómo utilizar eShell con sintaxis, prefijos, rutas de comandos, formas

abreviadas, alias, etc. Básicamente, es una guía rápida sobre eShell.

La próxima vez que ejecute eShell verá la siguiente pantalla:



NOTA: los comandos no distinguen entre mayúsculas y minúsculas. Puede usar letras en mayúscula o en minúscula y el comando se ejecutará igualmente.

Personalización de eShell

Puede personalizar eShell en el contexto `ui eshell`. Puede configurar el alias, los colores, el idioma, la directiva de ejecución de los scripts, puede optar por mostrar comandos ocultos, y establecer otros ajustes.

4.7.6.1 Uso

Sintaxis

Los comandos deben presentar una sintaxis correcta para funcionar y pueden constar de un prefijo, contexto, argumentos, opciones, etc. Esta es la sintaxis general que se utiliza en eShell:

[<prefijo>] [<ruta del comando>] <comando> [<argumentos>]

Ejemplo (este ejemplo activa la protección de documentos):

```
SET ANTIVIRUS DOCUMENT STATUS ENABLED
```

`SET:` un prefijo
`ANTIVIRUS DOCUMENT` ruta de acceso a un comando determinado, contexto al que pertenece dicho comando
`STATUS:` el comando propiamente dicho
`ENABLED:` argumento del comando

Si se utiliza `?` como argumento de un comando, se mostrará la sintaxis de dicho comando. Por ejemplo, el prefijo `STATUS ?` mostrará la sintaxis del comando `STATUS`:

SINTAXIS:

```
[get] | status
set status enabled | disabled
```

Verá que `[get]` se encierra entre corchetes. Esto indica que el prefijo `get` es el predeterminado para el comando `status`. De este modo, si se ejecuta `status` sin especificar ningún prefijo, se utilizará el prefijo predeterminado (en este caso, `get status`). El uso de comandos sin prefijos ahorra tiempo a la hora de escribir. Normalmente, `get:` es el prefijo predeterminado para la mayoría de los comandos; compruebe cuál es el prefijo predeterminado de un comando concreto para asegurarse de que es el que desea ejecutar.

NOTA: los comandos no distinguen mayúsculas y minúsculas, por lo que el uso de unas u otras no afectará a su

ejecución.

Prefijo/Operación
Un prefijo es una operación. El prefijo `GET` proporciona información sobre la configuración de una característica determinada de ESET Mail Security o muestra el estado (por ejemplo, `GET ANTIVIRUS STATUS` muestra el estado actual de la protección). El prefijo `SET` configura la funcionalidad o cambia su estado (`SET ANTIVIRUS STATUS ENABLED` activa la protección).

Estos son los prefijos que permite utilizar eShell. No todos los comandos admiten todos los prefijos:

`GET`: devuelve el estado o la configuración actual
`SET`: define el valor o el estado
`SELECT`: selecciona un elemento
`ADD`: añade un elemento
`REMOVE`: elimina un elemento
`CLEAR`: elimina todos los elementos o archivos
`START`: inicia una acción
`STOP`: detiene una acción
`PAUSE`: pone en pausa una acción
`RESUME`: reanuda una acción
`RESTORE`: restaura la configuración, el objeto o el archivo predeterminado
`SEND`: envía un objeto o archivo
`IMPORT`: importa desde un archivo
`EXPORT`: exporta a un archivo

Los prefijos como `GET` y `SET` se utilizan con muchos comandos; y algunos comandos, como `EXIT`, no utilizan ningún prefijo.

Ruta/contexto del comando
Los comandos se colocan en contextos que conforman una estructura de árbol. El nivel superior del árbol es la raíz. Cuando ejecuta eShell, el usuario está en el nivel raíz:

```
eShell>
```

Puede ejecutar el comando desde este nivel o introducir el nombre de contexto para desplazarse por el árbol. Por ejemplo, si introduce el contexto `TOOLS` , se mostrará una lista con todos los comandos y subcontextos disponibles desde este nivel.

Los elementos amarillos son comandos que el usuario puede ejecutar y los elementos grises, subcontextos que puede especificar. U subcontexto contiene más comandos.

Si desea subir un nivel, escriba `..` (dos puntos). Por ejemplo, si se encuentra aquí:

```
eShell antivirus startup>
```

escriba `..` para subir nivel, a:

```
eShell antivirus>
```

Si desea volver al nivel raíz desde `eShell antivirus startup>` (dos niveles por debajo del nivel raíz), simplemente escriba `..  ..` (dos puntos, un espacio y otros dos puntos). Así, subirá dos niveles hasta el nivel raíz, en este caso. Utilice una barra invertida `\` para volver directamente a raíz desde cualquier nivel, sea cual sea el punto del árbol contextual en el que se encuentre. Si desea acceder a un contexto determinado de niveles superiores, simplemente use el número correspondiente de `..` necesario para acceder al nivel deseado, pero utilice el espacio como separador. Por ejemplo, si desea subir tres niveles, utilice `..  ..  ..`

La ruta de acceso es relativa al contexto actual. Si el comando se encuentra en el contexto actual, no especifique una ruta. Por ejemplo, para ejecutar `GET ANTIVIRUS STATUS` escriba:

`GET ANTIVIRUS STATUS` si se encuentra el contexto raíz (en la línea de comandos se muestra `eShell>`)
`GET STATUS:` si se encuentra el contexto `ANTIVIRUS` (la línea de comandos muestra `eShell antivirus>`)
`.. GET STATUS:` si se encuentra el contexto `ANTIVIRUS STARTUP` (la línea de comandos muestra `eShell antivirus startup>`)

NOTA: puede usar un solo `.` (punto) en lugar de dos `..` porque un punto es la abreviatura de los dos puntos. Por ejemplo:

`. GET STATUS:` : si se encuentra en el contexto `ANTIVIRUS STARTUP` (la línea de comandos muestra `eShell antivirus startup>`)

Argumento
Un argumento es una acción que se realiza para un comando determinado. Por ejemplo, el comando `CLEAN-LEVEL` (situado en `ANTIVIRUS REALTIME ENGINE`) se puede utilizar con los argumentos siguientes:

`no` : Sin desinfección
`normal:` : Desinfección normal
`strict` desinfección exhaustiva

Otro ejemplo son los argumentos `ENABLED` o `DISABLED`, que se utilizan para activar o desactivar una función o característica determinadas.

Forma abreviada/comandos abreviados
eShell le permite acortar los contextos, comandos y argumentos (siempre que el argumento sea un modificador o una opción alternativa). Los argumentos o prefijos que sean un valor concreto, como un número, un nombre o una ruta de acceso, no se pueden acortar.

Ejemplos de formas abreviadas:

`set status enabled` => `set stat en`
`add antivirus common scanner-excludes C:\path\file.ext` => `add ant com scann C:\path\file.ext`

Si dos comandos o contextos empiezan con las mismas letras (por ejemplo `ABOUT` y `ANTIVIRUS`, y escribe `A` como comando abreviado), eShell no podrá decidir cuál de los dos comandos desea ejecutar y se mostrará un mensaje de error con los comandos que empiezan por "A" que puede elegir:

```
eShell>a
Este comando no es único: a

En este contexto, están disponibles los comandos siguientes:
ABOUT: muestra información sobre el programa
ANTIVIRUS: cambios en el contexto de antivirus
```

Al añadir una o más letras (por ejemplo, `AB` en vez de solo `A`) eShell ejecutará el comando `ABOUT` , que ahora es único.

NOTA: para asegurarse de que un comando se ejecuta tal como lo necesita, es preferible que no abrevie los comandos, argumentos y demás, sino que utilice la forma completa. De esta manera, el comando se ejecutará tal

como desea y no se producirán errores inesperados. Este consejo es especialmente útil para los scripts y archivos por lotes.

Finalización automática
Esta es una función nueva de eShell disponible desde la versión 2.0. Se trata de una función muy similar a la finalización automática disponible en el símbolo del sistema de Windows. Mientras que el símbolo del sistema de Windows completa las rutas de acceso a archivos, eShell completa también los comandos, los contextos y los nombres de operaciones. No permite la finalización de argumentos. Al escribir un comando, simplemente pulse la tecla Tabulador para completar o recorrer las distintas opciones. Pulse Mayúsculas + Tabulador para recorrer las opciones en sentido inverso. No se permite la combinación de formato abreviado y de finalización automática; elija qué función desea usar. Por ejemplo, cuando escribe `antivir real scan` y pulsa la tecla Tabulador no ocurre nada. En lugar de ello, escriba `antivir` y use la tecla Tabulador para completar `antivirus`, siga escribiendo real + Tabulador y scan + Tabulador. Desde ese punto podrá recorrer todas las opciones disponibles: scan-create, scan-execute, scan-open, etc.

Alias
Un alias es un nombre alternativo que se puede utilizar para ejecutar un comando (siempre que el comando tenga un alias asignado). Hay varios alias predeterminados:

`(global) close`: cerrar
`(global) quit`: cerrar
`(global) bye`: cerrar
`warnlog`: sucesos de registro de herramientas
`virlog`: detecciones de registro de herramientas
`antivirus on-demand log` : análisis de registro de herramientas

"(global)" significa que el comando se puede utilizar en cualquier sitio, independientemente del contexto actual. Un comando puede tener varios alias asignados; por ejemplo, el comando `EXIT` tiene los alias `CLOSE`, `QUIT` y `BYE`. Si desea cerrar eShell, puede utilizar el comando `EXIT` o cualquiera de sus alias. El alias `VIRLOG` es un alias para el comando `DETECTIONS` , que se encuentra en el contexto `TOOLS LOG` . De esta manera, el comando detections está disponible en el contexto `ROOT` y, por lo tanto, es más fácil acceder a él (no es necesario especificar `TOOLS` y, después, el contexto `LOG` para ejecutarlo directamente desde `ROOT`).

eShell le permite definir sus propios alias. Comando `ALIAS` se puede encontrar en el contexto `UI ESHELL` .

Configuración de la protección por contraseña
La configuración de ESET Mail Security puede protegerse por medio de una contraseña. Puede establecer la contraseña desde la interfaz gráfica de usuario o eShell por medio del comando `set ui access lock-password` . A partir de ese momento, tendrá que introducir la contraseña de forma interactiva con determinados comandos (como aquellos que cambian ajustes o modifican datos). Si tiene pensado trabajar con eShell durante un periodo de tiempo más prolongado y no desea tener que introducir la contraseña en varias ocasiones, puede configurar eShell para que recuerde la contraseña mediante el comando `set password` . La contraseña se especificará automáticamente para cada comando ejecutado que requiera contraseña. Se recordará hasta que salga de eShell; esto significa que tendrá que usar `set password` de nuevo cuando inicie una sesión nueva y quiera que eShell recuerde su contraseña.

Guía/Ayuda
Al ejecutar el comando `GUIDE` o `HELP` , se muestra la pantalla de primera ejecución, donde se explica cómo utilizar eShell. Este comando está disponible en el contexto `ROOT` (`eShell>`).

Historial de comandos
eShell guarda el historial de los comandos ejecutados. Este historial solo incluye la sesión interactiva actual de eShell, y se borrará cuando salga de eShell. Utilice las teclas de flecha arriba y abajo del teclado para desplazarse por el historial. Una vez que haya encontrando el comando que buscaba, puede volver a ejecutarlo o modificarlo sin necesidad de escribir el comando completo desde el principio.

CLS/Borrar pantalla
El comando `CLS` se puede utilizar para borrar la pantalla; funciona igual que la ventana de símbolo del sistema de Windows u otras interfaces de línea de comandos similares.

EXIT/CLOSE/QUIT/BYE
Para cerrar o salir de eShell, puede utilizar cualquiera de estos comandos (`EXIT`, `CLOSE`, `QUIT` o `BYE`).

4.7.6.2 Comandos

En esta sección se ofrece una lista de algunos comandos básicos de eShell con su descripción a modo de ejemplo.

NOTA: los comandos no distinguen mayúsculas y minúsculas, por lo que el uso de unas u otras no afectará a su ejecución.

Comandos de ejemplo (del contexto ROOT):

ABOUT

Muestra información sobre el programa. Indica el nombre del producto instalado, el número de versión, los componentes instalados (incluido el número de versión de cada componente) e información básica sobre el servidor y el sistema operativo en el que se está ejecutando ESET Mail Security.

RUTA DE ACCESO AL CONTEXTO:

```
root
```

CONTRASEÑA

Normalmente, para ejecutar comandos protegidos mediante contraseña es necesario introducir una contraseña por cuestiones de seguridad. Esto es así en comandos como, por ejemplo, los que desactivan la protección antivirus o los que pueden afectar a la funcionalidad de ESET Mail Security. La contraseña se le solicitará cada vez que ejecute el comando. Puede definir esta contraseña para no tener que introducirla cada vez. eShell recordará la contraseña y la utilizará automáticamente cuando se ejecute un comando protegido con contraseña. De esta manera, no tendrá que introducir la contraseña cada vez.

NOTA: la contraseña definida solo sirve para la sesión interactiva actual de eShell; se borrará cuando salga de eShell. La próxima vez que inicie eShell, tendrá que definir la contraseña de nuevo.

Esta contraseña definida también es muy útil a la hora de ejecutar scripts o archivos por lotes. A continuación se proporciona un ejemplo de archivo por lotes:

```
eshell start batch "&" set password plain <yourpassword> "&" set status disabled
```

Este comando concatenado inicia el modo por lotes, define la contraseña y desactiva la protección.

RUTA DE ACCESO AL CONTEXTO:

```
root
```

SINTAXIS:

```
[get] | restore password
```

```
set password [plain <password>]
```

OPERACIONES:

`get`: muestra la contraseña

`set`: establece o borra la contraseña

`restore`: borra la contraseña

ARGUMENTOS:

`plain`: cambia al modo de introducción de contraseña como parámetro

`contraseña` contraseña

EJEMPLOS:

`set password plain <yourpassword>` establece una contraseña para los comandos protegidos mediante contraseña

`restore password`: borra la contraseña

EJEMPLOS:

`get password`: utilice este comando para comprobar si hay una contraseña configurada (solo se muestran asteriscos "*", no la contraseña); si no se muestra ningún asterisco, significa que no hay ninguna contraseña definida

`set password plain <yourpassword>` utilice este comando para establecer la contraseña definida

`restore password`: este comando borra la contraseña definida

STATUS

Muestra información sobre el estado de la protección actual de ESET Mail Security (similar a la GUI).

RUTA DE ACCESO AL CONTEXTO:

`root`

SINTAXIS:

`[get] | restore status`

`set status disabled | enabled`

OPERACIONES:

`get`: muestra el estado de la protección antivirus

`set`: activa o desactiva la protección antivirus

`restore`: restaura la configuración predeterminada

ARGUMENTOS:

`desactivada` desactiva la protección antivirus

`enabled`: activa la protección antivirus

EJEMPLOS:

`get status`: muestra el estado de la protección actual

`set status disabled`: desactiva la protección

`restore status`: restaura la configuración predeterminada de la protección (Activada)

VIRLOG

Este es un alias del comando `DETECTIONS` . es útil cuando se necesita ver información sobre las amenazas detectadas.

WARNLOG

Este es un alias del comando `EVENTS` . es útil cuando se necesita ver información sobre varios sucesos.

4.7.6.3 Archivos por lotes/Creación de scripts

Puede usar eShell como una potente herramienta de creación de scripts para la automatización de tareas. Si desea usar un archivo por lotes con eShell, créelo con eShell y especifique comandos en él. Por ejemplo:

```
eshell get antivirus status
```

También puede encadenar comandos, tarea a veces necesaria. Por ejemplo, si quiere obtener un tipo de tarea programada determinado, introduzca lo siguiente:

```
eshell select scheduler task 4 "&" get scheduler action
```

La selección del elemento (tarea número 4 en este caso) normalmente se aplica solo a una instancia actualmente en ejecución de eShell. Si ejecutara estos dos comandos sucesivamente, el segundo comando fallaría y presentaría el error "No hay ninguna tarea seleccionada o la tarea seleccionada ya no existe".

Por motivos de seguridad, la directiva de ejecución está ajustada como Scripts limitados de forma predeterminada. Esta configuración le permite usar eShell como herramienta de supervisión, pero no le permitirá efectuar cambios en la configuración de ESET Mail Security. Al especificar comandos que puedan afectar a la seguridad, como aquellos que desactivan la protección, se le mostrará el mensaje **Acceso denegado**. Para poder ejecutar los comandos que realizan cambios en la configuración, le recomendamos que use archivos por lotes firmados.

Si por algún motivo necesita poder cambiar la configuración mediante la introducción de un comando en el símbolo del sistema de Windows, deberá conceder a eShell acceso total (no se recomienda). Para conceder acceso total, utilice el comando `ui eshell shell-execution-policy` en el modo interactivo de eShell, o hágalo a través de la interfaz gráfica de usuario en la opción **Configuración avanzada** > **Interfaz de usuario** > ESET Shell.

Archivos por lotes firmados
eShell le permite proteger archivos por lotes comunes (*.bat) por medio de una firma. Los scripts se firman con la misma contraseña que se usa para la protección de la configuración. Para poder firmar un script debe activar primero la protección de la configuración. Puede hacerlo desde la interfaz gráfica de usuario o desde eShell con el comando `set ui access lock-password`. Una vez configurada la contraseña de protección de la configuración podrá empezar a firmar archivos por lotes.

Para firmar un archivo por lotes, ejecute `sign <script.bat>` desde el contexto raíz de eShell, donde *script.bat* es la ruta de acceso al script que desea firmar. Introduzca y confirme la contraseña que se utilizará para la firma. Esta contraseña debe coincidir con la contraseña de protección de la configuración. La firma se coloca al final del archivo por lotes con formato comentado. Si este script se ha firmado anteriormente, la firma se sustituirá por una nueva.

NOTA: si se modifica un archivo por lotes previamente firmado, tendrá que firmarlo de nuevo.

NOTA: si cambia la contraseña de protección de la configuración, tendrá que firmar todos los scripts de nuevo, o su ejecución fallará desde el momento en el que haya cambiado la contraseña de protección de la configuración. Esto se debe a que la contraseña introducida al firmar el script debe coincidir con la contraseña de protección de la configuración del sistema de destino.

Para ejecutar un archivo por lotes firmado desde el símbolo del sistema de Windows o como tarea programada, utilice el siguiente comando:

```
eshell run <script.bat>
```

donde script.bat es la ruta de acceso al archivo por lotes. Por ejemplo `eshell run d:\miscripteshell.bat`

4.7.7 ESET SysInspector

ESET SysInspector es una aplicación que inspecciona a fondo el ordenador, recopila información detallada sobre los componentes del sistema (como los controladores y aplicaciones instalados, las conexiones de red o las entradas importantes del registro) y evalúa el nivel de riesgo de cada componente. Esta información puede ayudar a determinar la causa de un comportamiento sospechoso del sistema, que puede deberse a una incompatibilidad de software o hardware o a una infección de código malicioso.

En la ventana de ESET SysInspector se muestra la siguiente información de los registros creados:

- **Fecha y hora**: fecha y hora de creación del registro.
- **Comentario**: breve comentario.
- **Usuario**: nombre del usuario que creó el registro.
- **Estado**: estado de la creación del registro.

Están disponibles las siguientes acciones:

- **Abrir**: abre el registro creado. También puede abrirlo al hacer clic con el botón derecho en el registro creado y, a continuación, seleccionar **Mostrar** en el menú contextual.
- **Comparar**: compara dos registros existentes.
- **Crear**: crea un registro nuevo. Espere hasta que el registro de ESET SysInspector esté completo (**Estado**: Creado).
- **Eliminar**: elimina de la lista los registros seleccionados.

Al hacer clic con el botón derecho del ratón en uno o varios de los registros seleccionados se mostrarán las siguientes opciones del menú contextual:

- **Mostrar**: abre el registro seleccionado en ESET SysInspector (igual que al hacer doble clic en un registro).
- **Comparar**: compara dos registros existentes.
- **Crear**: crea un registro nuevo. Espere hasta que el registro de ESET SysInspector esté completo (**Estado**: Creado).
- **Eliminar**: elimina de la lista los registros seleccionados.
- **Eliminar todos**: elimina todos los registros.
- **Exportar**: exporta el registro a un archivo *.xml* o *.xml* comprimido.

4.7.7.1 Crear un informe del estado del sistema

Escriba un breve comentario que describa el registro que se creará y haga clic en el botón **Agregar**. Espere hasta que el registro de ESET SysInspector esté completo (estado Creado). La creación del registro podría llevar cierto tiempo, en función de la configuración de hardware y de los datos del sistema.

4.7.7.2 ESET SysInspector

4.7.7.2.1 Introducción a ESET SysInspector

ESET SysInspector es una aplicación que examina el ordenador a fondo y muestra los datos recopilados de forma exhaustiva. Información como los controladores y aplicaciones instalados, las conexiones de red o entradas de registro importantes pueden ayudarle a investigar el comportamiento sospechoso del sistema debido a la incompatibilidad de software o hardware o a la infección de código malicioso.

Puede acceder a ESET SysInspector de dos formas: desde la versión integrada en las soluciones ESET Security o descargando la versión independiente (SysInspector.exe) del sitio web de ESET de forma gratuita. Las dos versiones tienen una función idéntica y los mismos controles del programa. Solo se diferencian en el modo de gestión de los resultados. Tanto la versión independiente como la versión integrada le permiten exportar instantáneas del sistema en un archivo *.xml* y guardarlas en el disco. No obstante, la versión integrada también le permite almacenar las instantáneas del sistema directamente en **Herramientas** > **ESET SysInspector** (excepto ESET Remote Administrator). Para obtener más información, consulte la sección ESET SysInspector como parte de ESET Mail Security.

ESET SysInspector tardará un rato en analizar el ordenador; el tiempo necesario puede variar entre 10 segundos y unos minutos, según la configuración de hardware, el sistema operativo y el número de aplicaciones instaladas en el ordenador.

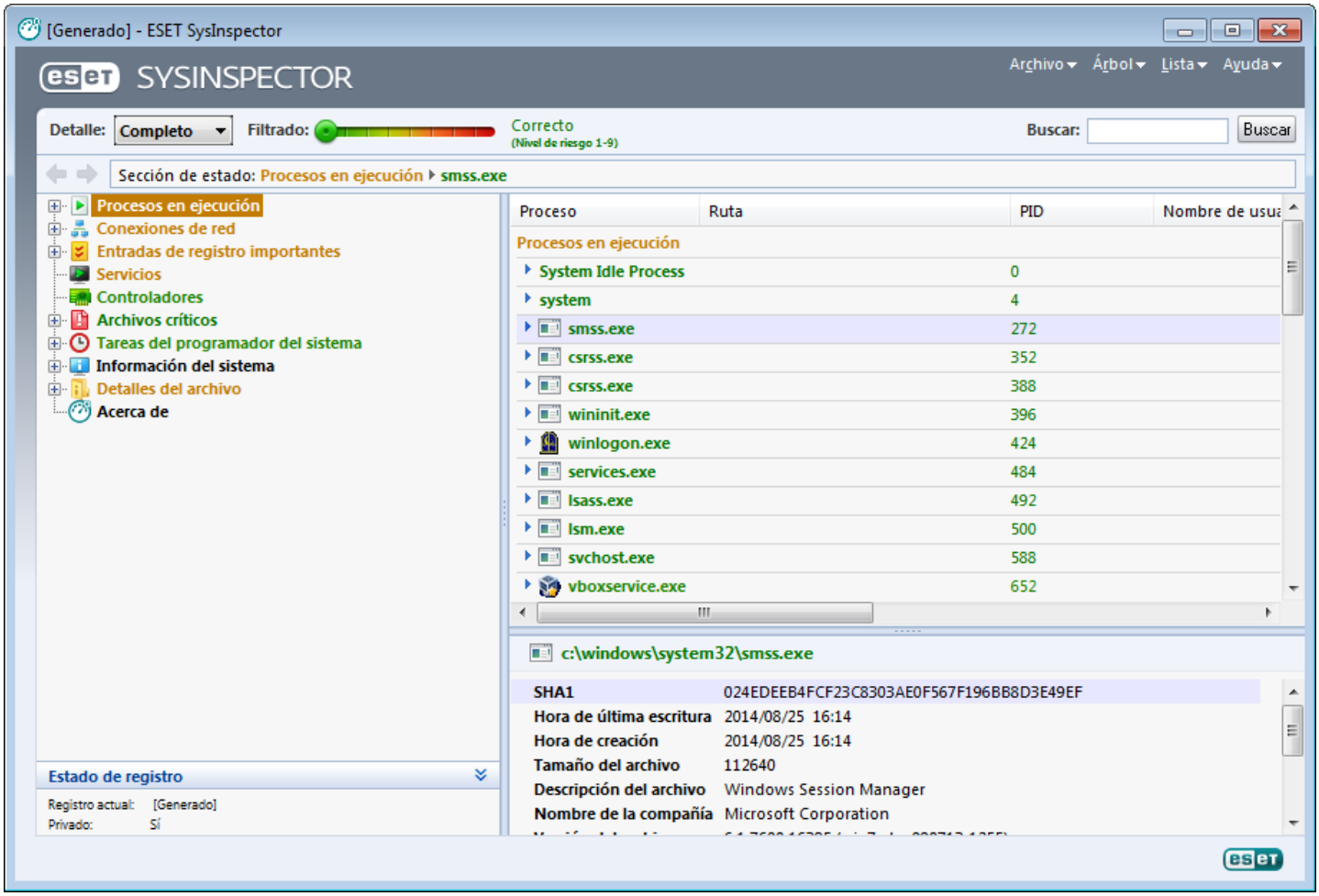
4.7.7.2.1.1 Inicio de ESET SysInspector

Para iniciar ESET SysInspector simplemente tiene que ejecutar el archivo *SysInspector.exe* que descargó del sitio web de ESET. Si ya tiene instalada alguna de las soluciones de ESET Security, puede ejecutar ESET SysInspector directamente desde el menú Inicio (haga clic en **Programas** > **ESET** > **ESET Mail Security**).

Espere mientras la aplicación examina el sistema. El proceso de inspección puede tardar varios minutos.

4.7.7.2.2 Interfaz de usuario y uso de la aplicación

Para un uso sencillo, la ventana principal del programa se divide en cuatro secciones: Controles de programa, en la parte superior de la ventana principal del programa; la ventana de navegación, situada a la izquierda; la ventana Descripción, situada a la derecha; y la ventana Detalles, situada en la parte inferior de la ventana principal. En la sección Estado de registro se enumeran los parámetros básicos de un registro (filtro utilizado, tipo de filtro, si el registro es resultado de una comparación, etc.).



4.7.7.2.2.1 Controles de programa

Esta sección contiene la descripción de todos los controles de programa disponibles en ESET SysInspector.

Archivo

Al hacer clic en **Archivo**, puede guardar el estado actual del sistema para examinarlo más tarde o abrir un registro guardado anteriormente. Para la publicación, es recomendable que genere un registro **Para enviar**. De esta forma, el registro omite la información confidencial (nombre del usuario actual, nombre del ordenador, nombre del dominio, privilegios del usuario actual, variables de entorno, etc.).

NOTA: los informes almacenados de ESET SysInspector se pueden abrir previamente arrastrándolos y soltándolos en la ventana principal del programa.

Árbol

Le permite expandir o cerrar todos los nodos, y exportar las secciones seleccionadas al script de servicio.

Lista

Contiene funciones para una navegación más sencilla por el programa y otras funciones como, por ejemplo, la búsqueda de información en línea.

Ayuda

Contiene información sobre la aplicación y sus funciones.

Detalle

Este ajuste modifica la información mostrada en la ventana principal del programa para que pueda trabajar con ella más fácilmente. El modo "Básico", le permite acceder a la información utilizada para buscar soluciones a problemas comunes del sistema. En el modo "Medio", el programa muestra menos detalles. En el modo "Completo", ESET SysInspector muestra toda la información necesaria para solucionar problemas muy específicos.

Filtrado

Es la mejor opción para buscar entradas de registro o archivos sospechosos en el sistema. Ajuste el control deslizante para filtrar los elementos por su nivel de riesgo. Si el control deslizante se coloca lo más a la izquierda posible (nivel de riesgo 1), se mostrarán todos los elementos. Al mover el control deslizante a la derecha, el programa filtra todos los elementos que tienen un nivel de riesgo inferior al actual y muestra solo los elementos con un nivel de sospecha superior al mostrado. Si el control deslizante está colocado lo más a la derecha posible, el programa mostrará solo los elementos dañinos conocidos.

Todos los elementos que tengan un nivel de riesgo entre 6 y 9 pueden constituir un riesgo de seguridad. Si utiliza una solución de seguridad de ESET, le recomendamos que analice su sistema con ESET Online Scanner cuando ESET SysInspector encuentre un elemento de este tipo. ESET Online Scanner es un servicio gratuito.

NOTA: el nivel de riesgo de un elemento se puede determinar rápidamente comparando el color del elemento con el color del control deslizante de nivel de riesgo.

Comparar

Cuando se comparan dos registros, puede elegir que se visualicen todos los elementos, solo los elementos agregados, solo los elementos eliminados y solo los elementos sustituidos.

Buscar

Esta opción se puede utilizar para buscar rápidamente un elemento específico por su nombre completo o parcial. Los resultados de la solicitud de búsqueda aparecerán en la ventana Descripción.

Retorno

Al hacer clic en las flechas hacia atrás o hacia delante, puede volver a la información mostrada previamente en la ventana Descripción. Puede utilizar la tecla Retroceso y la tecla de espacio, en lugar de hacer clic en las flechas atrás y adelante.

Sección de estado

Muestra el nodo actual en la ventana de navegación.

Importante: los elementos destacados en rojo son elementos desconocidos, por eso el programa los marca como potencialmente peligrosos. Que un elemento aparezca marcado en rojo no significa que deba eliminar el archivo. Antes de eliminarlo, asegúrese de que el archivo es realmente peligroso o innecesario.

4.7.7.2.2.2 Navegación por ESET SysInspector

ESET SysInspector divide los tipos de información en distintas secciones básicas denominadas nodos. Si está disponible, puede encontrar información adicional expandiendo cada uno de los nodos en subnodos. Para abrir o contraer un nodo, haga doble clic en el nombre del nodo o haga clic en + o −, junto al nombre del nodo. A medida que explora la estructura de árbol de nodos y subnodos en la ventana de navegación, encontrará información variada de cada nodo en la ventana Descripción. Si examina los elementos en la ventana Descripción, es posible que se muestre información adicional de cada uno de los elementos en la ventana Detalles.

A continuación, se encuentran las descripciones de los nodos principales de la ventana de navegación e información relacionada en las ventanas Descripción y Detalles.

Procesos en ejecución

Este nodo contiene información sobre las aplicaciones y los procesos que se ejecutan al generar el registro. En la ventana Descripción, puede encontrar información adicional de cada proceso como, por ejemplo, bibliotecas dinámicas utilizadas por el proceso y su ubicación en el sistema, el nombre del proveedor de la aplicación, el nivel de riesgo del archivo, etc.

La ventana Detalles contiene información adicional de los elementos seleccionados en la ventana Descripción como, por ejemplo, el tamaño del archivo o su hash.

NOTA: un sistema operativo incluye varios componentes kernel importantes que se ejecutan constantemente y proporcionan funciones básicas y esenciales para otras aplicaciones de usuario. En determinados casos, estos procesos aparecen en la herramienta ESET SysInspector con una ruta de archivo que comienza por \??\. Estos símbolos proporcionan optimización de prelanzamiento de esos procesos; son seguros para el sistema; son seguros para el sistema.

Conexiones de red

La ventana Descripción contiene una lista de procesos y aplicaciones que se comunican a través de la red utilizando el protocolo seleccionado en la ventana de navegación (TCP o UDP), así como la dirección remota a la que se conecta la aplicación. También puede comprobar las direcciones IP de los servidores DNS.

La ventana Detalles contiene información adicional de los elementos seleccionados en la ventana Descripción como, por ejemplo, el tamaño del archivo o su hash.

Entradas de registro importantes

Contiene una lista de entradas de registro seleccionadas que suelen estar asociadas a varios problemas del sistema, como las que especifican programas de arranque, objetos auxiliares del navegador (BHO), etc.

En la ventana Descripción, puede encontrar los archivos que están relacionados con entradas de registro específicas. Puede ver información adicional en la ventana Detalles.

Servicios

La ventana Descripción contiene una lista de archivos registrados como Windows Services (Servicios de Windows). En la ventana Detalles, puede consultar el modo de inicio definido para el servicio e información específica del archivo.

Controladores

Una lista de los controladores instalados en el sistema.

Archivos críticos

En la ventana Descripción se muestra el contenido de los archivos críticos relacionados con el sistema operativo Microsoft Windows.

Tareas del programador del sistema

Contiene una lista de tareas desencadenadas por el Programador de tareas de Windows a una hora o con un intervalo de tiempo especificados.

Información del sistema

Contiene información detallada sobre el hardware y el software, así como información sobre las variables de entorno, los derechos de usuario establecidos y registros de sucesos del sistema.

Detalles del archivo

Una lista de los archivos del sistema importantes y los archivos de la carpeta Archivos de programa. Encontrará información adicional específica de los archivos en las ventanas Descripción y Detalles.

Acerca de...

Información sobre la versión de ESET SysInspector y la lista de módulos de programa.

Los accesos directos que se pueden utilizar en ESET SysInspector son:

Archivo

Ctrl + O	abre el registro existente
Ctrl + S	guarda los registros creados

Generar

Ctrl + G	genera una instantánea estándar del estado del ordenador
Ctrl + H	genera una instantánea del estado del ordenador que también puede registrar información confidencial

Filtrado de elementos

1, O	seguro, se muestran los elementos que tienen un nivel de riesgo de 1 a 9
2	seguro, se muestran los elementos que tienen un nivel de riesgo de 2 a 9
3	seguro, se muestran los elementos que tienen un nivel de riesgo de 3 a 9
4, U	desconocido, se muestran los elementos que tienen un nivel de riesgo de 4 a 9
5	desconocido, se muestran los elementos que tienen un nivel de riesgo de 5 a 9
6	desconocido, se muestran los elementos que tienen un nivel de riesgo de 6 a 9
7, B	peligroso, se muestran los elementos que tienen un nivel de riesgo de 7 a 9
8	peligroso, se muestran los elementos que tienen un nivel de riesgo de 8 a 9
9	peligroso, se muestran los elementos que tienen un nivel de riesgo de 9
-	disminuye el nivel de riesgo
+	aumenta el nivel de riesgo
Ctrl + 9	modo de filtrado, nivel igual o mayor
Ctrl + 0	modo de filtrado, nivel igual únicamente

Ver

Ctrl + 5	ver por proveedor, todos los proveedores
Ctrl + 6	ver por proveedor, solo Microsoft
Ctrl + 7	ver por proveedor, todos los demás proveedores
Ctrl + 3	muestra todos los detalles
Ctrl + 2	muestra la mitad de los detalles
Ctrl + 1	visualización básica
Retroceso	retrocede un espacio
Espacio	avanza un espacio
Ctrl + W	expande el árbol
Ctrl + Q	contrae el árbol

Otros controles

Ctrl + T	va a la ubicación original del elemento tras seleccionarlo en los resultados de búsqueda
Ctrl + P	muestra información básica sobre un elemento
Ctrl + A	muestra toda la información sobre un elemento
Ctrl + C	copia el árbol del elemento actual

Ctrl + X	copia elementos
Ctrl + B	busca información en Internet acerca de los archivos seleccionados
Ctrl + L	abre la carpeta en la que se encuentra el archivo seleccionado
Ctrl + R	abre la entrada correspondiente en el editor de registros
Ctrl + Z	copia una ruta de acceso a un archivo (si el elemento está asociado a un archivo)
Ctrl + F	activa el campo de búsqueda
Ctrl + D	cierra los resultados de búsqueda
Ctrl + E	ejecuta el script de servicio

Comparación

Ctrl + Alt + O	abre el registro original/comparativo
Ctrl + Alt + R	cancela la comparación
Ctrl + Alt + 1	muestra todos los elementos
Ctrl + Alt + 2	muestra solo los elementos agregados, el registro mostrará los elementos presentes en el registro actual
Ctrl + Alt + 3	muestra solo los elementos eliminados, el registro mostrará los elementos presentes en el registro anterior
Ctrl + Alt + 4	muestra solo los elementos sustituidos (archivos incluidos)
Ctrl + Alt + 5	muestra solo las diferencias entre registros
Ctrl + Alt + C	muestra la comparación
Ctrl + Alt + N	muestra el registro actual
Ctrl + Alt + P	abre el registro anterior

Varios

F1	ver ayuda
Alt + F4	cerrar programa
Alt + Shift + F4	cerrar programa sin preguntar
Ctrl + I	estadísticas de registro

4.7.7.2.2.3 Comparar

La característica Comparar permite al usuario comparar dos registros existentes. El resultado de esta característica es un conjunto de elementos no comunes a ambos registros. Esta herramienta permite realizar un seguimiento de los cambios introducidos en el sistema, una característica muy útil para la detección de código malicioso.

Una vez iniciada, la aplicación crea un registro nuevo, que aparecerá en una ventana nueva. Haga clic en **Archivo** > **Guardar registro** para guardar un registro en un archivo. Los archivos de registro se pueden abrir y ver posteriormente. Para abrir un registro existente, haga clic en **Archivo** > **Abrir registro**. En la ventana principal del programa, ESET SysInspector muestra siempre un registro a la vez.

La comparación de dos registros le permite ver simultáneamente un registro activo y un registro guardado en un archivo. Para comparar registros, haga clic en **Archivo** > **Comparar registros** y elija **Seleccionar archivo**. El registro seleccionado se comparará con el registro activo en la ventana principal del programa. El registro comparativo solo muestra las diferencias entre los dos registros.

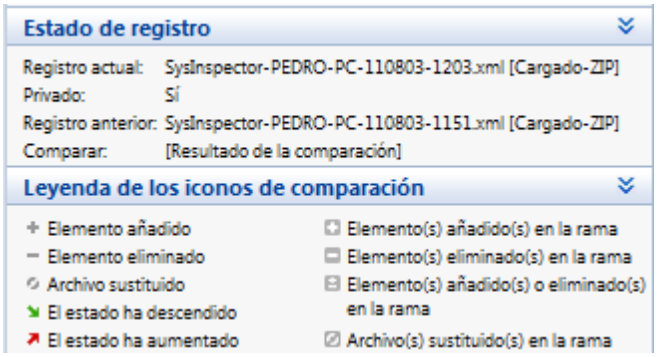
NOTA: si compara dos archivos de registro, haga clic en **Archivo** > **Guardar registro** para guardarlo como archivo ZIP. Se guardarán ambos archivos. Si abre posteriormente dicho archivo, los registros contenidos en el mismo se compararán automáticamente.

Junto a los elementos mostrados, ESET SysInspector muestra símbolos que identifican las diferencias entre los registros comparados.

Descripción de todos los símbolos que pueden aparecer junto a los elementos:

- Nuevo valor que no se encuentra en el registro anterior.
- La sección de estructura de árbol contiene valores nuevos.
- Valor eliminado que solo se encuentra en el registro anterior.
- La sección de estructura de árbol contiene valores eliminados.
- Se ha cambiado un valor o archivo.
- La sección de estructura de árbol contiene valores o archivos modificados.
- Ha disminuido el nivel de riesgo, o este era superior en el registro anterior.
- Ha aumentado el nivel de riesgo o era inferior en el registro anterior.

La explicación que aparece en la esquina inferior izquierda describe todos los símbolos, además de mostrar los nombres de los registros que se están comparando.


Estado de registro
Registro actual: SysInspector-PEDRO-PC-110803-1203.xml [Cargado-ZIP]
Privado: Sí
Registro anterior: SysInspector-PEDRO-PC-110803-1151.xml [Cargado-ZIP]
Comparar: [Resultado de la comparación]
Leyenda de los iconos de comparación
Elemento añadido
Elemento eliminado
Archivo sustituido
El estado ha descendido
El estado ha aumentado
Elemento(s) añadido(s) en la rama
Elemento(s) eliminado(s) en la rama
Elemento(s) añadido(s) o eliminado(s) en la rama
Archivo(s) sustituido(s) en la rama

Los registros comparativos se pueden guardar en un archivo para consultarlos más adelante.

Ejemplo

Genere y guarde un registro, que incluya información original sobre el sistema, en un archivo con el nombre previo.xml. Tras realizar los cambios en el sistema, abra ESET SysInspector y deje que genere un nuevo registro. Guárdelo en un archivo con el nombre *actual.xml*.

Para realizar un seguimiento de los cambios entre estos dos registros, haga clic en **Archivo** > **Comparar registros**. El programa creará un registro comparativo con las diferencias entre ambos registros.

Se puede lograr el mismo resultado con la siguiente opción de la línea de comandos:

SysIsnpector.exe actual.xml previo.xml

4.7.7.2.3 Parámetros de la línea de comandos

ESET SysInspector admite la generación de informes desde la línea de comandos con estos parámetros:

/gen	genera un registro directamente desde la línea de comandos, sin ejecutar la interfaz gráfica.
/privacy	genera un registro omitiendo la información personal.
/zip	guarda el registro obtenido en un archivo comprimido zip.
/silent	cancela la ventana de progreso cuando se genera un registro desde la línea de comandos.
/blank	inicia ESET SysInspector sin generar o cargar un registro.

Ejemplos

Uso:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Para cargar un registro determinado directamente en el navegador, utilice: *SysInspector.exe .\clientlog.xml*
Para generar un registro desde la línea de comandos, utilice: *SysInspector.exe /gen=.\mynewlog.xml*
Para generar un registro que no incluya la información confidencial directamente como archivo comprimido, utilice: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Para comparar dos archivos de registro y examinar las diferencias, utilice: *SysInspector.exe new.xml old.xml*

NOTA: si el nombre del archivo o la carpeta contiene un espacio, debe escribirse entre comillas.

4.7.7.2.4 Script de servicio

El script de servicio es una herramienta que ayuda a los clientes que utilizan ESET SysInspector eliminando fácilmente del sistema los objetos no deseados.

El script de servicio permite al usuario exportar el registro completo de ESET SysInspector o las partes que seleccione. Después de exportarlo, puede marcar los objetos que desea eliminar. A continuación, puede ejecutar el registro modificado para eliminar los objetos marcados.

El script de servicio es ideal para los usuarios avanzados con experiencia previa en el diagnóstico de problemas del sistema. Las modificaciones realizadas por usuarios sin experiencia pueden provocar daños en el sistema operativo.

Ejemplo

Si sospecha que el ordenador está infectado por un virus que el antivirus no detecta, siga estas instrucciones:

1. Ejecute ESET SysInspector para generar una nueva instantánea del sistema.
2. Seleccione el primero y el último elemento de la sección de la izquierda (en la estructura de árbol) mientras mantiene pulsada la tecla Mayús.
3. Haga clic con el botón secundario en los objetos seleccionados y elija la opción **Exportar las secciones seleccionadas al script de servicio**.
4. Los objetos seleccionados se exportarán a un nuevo registro.
5. Este es el paso más importante de todo el procedimiento: abra el registro nuevo y cambie el atributo - a + para todos los objetos que desee eliminar. Asegúrese de que no ha marcado ningún archivo u objeto importante del sistema operativo.
6. Abra ESET SysInspector, haga clic en **Archivo** > **Ejecutar script de servicio** e introduzca la ruta del script.
7. Haga clic en **Aceptar** para ejecutar el script.

4.7.7.2.4.1 Generación de scripts de servicio

Para generar un script de servicio, haga clic con el botón derecho del ratón en cualquier elemento del árbol de menús (en el panel izquierdo) de la ventana principal de ESET SysInspector. En el menú contextual, seleccione **Exportar todas las secciones al script de servicio** o **Exportar secciones seleccionadas al script de servicio**.

NOTA: cuando se comparan dos registros, el script de servicio no se puede exportar.

4.7.7.2.4.2 Estructura del script de servicio

En la primera línea del encabezado del script encontrará información sobre la versión del motor (ev), la versión de la interfaz gráfica de usuario (gv) y la versión del registro (lv). Puede utilizar estos datos para realizar un seguimiento de los posibles cambios del archivo .xml que genere el script y evitar las incoherencias durante la ejecución. Esta parte del script no se debe modificar.

El resto del archivo se divide en secciones, donde los elementos se pueden modificar (indique los que procesará el script). Para marcar los elementos que desea procesar, sustituya el carácter "-" situado delante de un elemento por el carácter "+". En el script, las secciones se separan mediante una línea vacía. Cada sección tiene un número y un título.

01) Running processes (Procesos en ejecución)

En esta sección se incluye una lista de todos los procesos que se están ejecutando en el sistema. Cada proceso se identifica mediante su ruta UNC y, posteriormente, su código hash CRC16 representado mediante asteriscos (*).

Ejemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

En este ejemplo se ha seleccionado (marcado con el carácter "+") el proceso module32.exe, que finalizará al ejecutar el script.

02) Loaded modules (Módulos cargados)

En esta sección se listan los módulos del sistema que se utilizan actualmente.

Ejemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

En este ejemplo, se marcó el módulo khbekhb.dll con el signo "+". Cuando se ejecute, el script reconocerá los procesos mediante el módulo específico y los finalizará.

03) TCP connections (Conexiones TCP)

En esta sección se incluye información sobre las conexiones TCP existentes.

Ejemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Cuando se ejecute, el script localizará al propietario del socket en las conexiones TCP marcadas y detendrá el socket, liberando así recursos del sistema.

04) UDP endpoints (Puntos finales UDP)

En esta sección se incluye información sobre los puntos finales UDP.

Ejemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Cuando se ejecute, el script aislará al propietario del socket en los puntos finales UDP marcados y detendrá el socket.

05) DNS server entries (Entradas del servidor DNS)

En esta sección se proporciona información sobre la configuración actual del servidor DNS.

Ejemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Las entradas marcadas del servidor DNS se eliminarán al ejecutar el script.

06) Important registry entries (Entradas de registro importantes)

En esta sección se proporciona información sobre las entradas de registro importantes.

Ejemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Cuando se ejecute el script, las entradas marcadas se eliminarán, reducirán a valores de 0 bytes o restablecerán en sus valores predeterminados. La acción realizada en cada entrada depende de su categoría y del valor de la clave en el registro específico.

07) Services (Servicios)

En esta sección se listan los servicios registrados en el sistema.

Ejemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Cuando se ejecute el script, los servicios marcados y los servicios dependientes se detendrán y desinstalarán.

08) Drivers (Controladores)

En esta sección se listan los controladores instalados.

Ejemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Al ejecutar el script, las unidades seleccionadas se detendrán. Tenga en cuenta que algunas unidades no se permitirán a sí mismas detenerse.

09) Critical files (Archivos críticos)

En esta sección se proporciona información sobre los archivos críticos para el correcto funcionamiento del sistema operativo.

Ejemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Los elementos seleccionados se eliminarán o restablecerán en sus valores originales.

4.7.7.2.4.3 Ejecución de scripts de servicio

Seleccione todos los elementos que desee y, a continuación, guarde y cierre el script. Ejecute el script modificado directamente desde la ventana principal de ESET SysInspector, con la opción **Ejecutar script de servicio** del menú Archivo. Cuando abra un script, el programa mostrará el mensaje siguiente: **¿Está seguro de que desea ejecutar el script de servicio "%Scriptname%"?** Una vez que haya confirmado la selección, es posible que se muestre otra advertencia para informarle de que el script de servicio que intenta ejecutar no está firmado. Haga clic en **Ejecutar** para iniciar el script.

Se abrirá un cuadro de diálogo para indicarle que el script se ha ejecutado correctamente.

Si el script no se puede procesar por completo, se mostrará un cuadro de diálogo con el mensaje siguiente: **El script de servicio se ejecutó parcialmente. ¿Desea ver el informe de errores?** Seleccione **Sí** para ver un informe de errores completo con todas las operaciones que no se ejecutaron.

Si no se reconoce el script, aparece un cuadro de diálogo con el mensaje siguiente: **No se ha firmado el script de servicio seleccionado. La ejecución de scripts desconocidos y sin firmar podría dañar seriamente los datos del ordenador. ¿Está seguro de que desea ejecutar el script y llevar a cabo las acciones?** Esto podría deberse a que el script presenta incoherencias (encabezado dañado, título de sección dañado, falta línea vacía entre secciones, etc.). Vuelva a abrir el archivo del script y corrija los errores o cree un script de servicio nuevo.

4.7.7.2.5 Preguntas frecuentes

¿Es necesario contar con privilegios de administrador para ejecutar ESET SysInspector?

ESET SysInspector no requiere privilegios de administrador para su ejecución, pero sí es necesario utilizar una cuenta de administrador para acceder a parte de la información que recopila. Si lo ejecuta como usuario estándar o usuario restringido, se recopilará menos información sobre su entorno operativo.

¿ESET SysInspector crea archivos de registro?

ESET SysInspector puede crear un archivo de registro de la configuración de su ordenador. Para guardar uno, haga clic en **Archivo** > **Guardar registro** en el menú principal. Los registros se guardar con formato XML. Por defecto, los archivos se guardan en el directorio *%USERPROFILE%\My Documents*, con una convención de nombre de archivo de "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". Si lo desea, puede modificar tanto la ubicación como el nombre del archivo de registro antes de guardarlo.

¿Cómo puedo ver el contenido del archivo de registro de ESET SysInspector?

Para visualizar un archivo de registro creado por ESET SysInspector, ejecute la aplicación y haga clic en **Archivo** > **Abrir registro** en el menú principal del programa. También puede arrastrar y soltar los archivos de registro en la aplicación ESET SysInspector. Si necesita ver los archivos de registro de ESET SysInspector con frecuencia, le recomendamos que cree un acceso directo al archivo SYSINSPECTOR.EXE en su escritorio. Para ver los archivos de registro, arrástrelos y suéltelos en ese acceso directo. Por razones de seguridad, es posible que Windows Vista/7 no

permita la opción de arrastrar y soltar entre ventanas con permisos de seguridad distintos.

¿Hay una especificación disponible para el formato de archivo de registro? ¿Y un kit de desarrollo de software?

Actualmente, no se encuentra disponible ninguna especificación para el formato del archivo de registro, ni un conjunto de herramientas de programación, ya que la aplicación se encuentra aún en fase de desarrollo. Una vez que se haya lanzado, podremos proporcionar estos elementos en función de la demanda y los comentarios por parte de los clientes.

¿Cómo evalúa ESET SysInspector el riesgo que plantea un objeto determinado?

Generalmente, ESET SysInspector asigna un nivel de riesgo a los objetos (archivos, procesos, claves de registro, etc). Para esto, utiliza una serie de reglas heurísticas que examinan las características de cada uno de ellos y, después, pondera el potencial de actividad maliciosa. Según estas heurísticas, a los objetos se les asignará un nivel de riesgo desde el valor "1: seguro" (en color verde) hasta "9: peligroso" (en color rojo). En el panel de navegación que se encuentra a la izquierda, las secciones estarán coloreadas según el nivel máximo de peligrosidad que presente un objeto en su interior.

El nivel de riesgo "6: desconocido (en color rojo)", ¿significa que un objeto es peligroso?

Las evaluaciones de ESET SysInspector no garantizan que un objeto sea malicioso. Esta determinación deberá confirmarla un experto en seguridad informática. ESET SysInspector está diseñado para proporcionar una guía rápida a estos expertos, con la finalidad de que conozcan los objetos que deberían examinar en un sistema en busca de algún comportamiento inusual.

¿Por qué ESET SysInspector se conecta a Internet cuando se ejecuta?

Como muchas otras aplicaciones, ESET SysInspector contiene una firma digital que actúa a modo de "certificado". Esta firma sirve para garantizar que ESET ha desarrollado la aplicación y que no se ha alterado. Con el fin de comprobar la veracidad del certificado, el sistema operativo contacta con una autoridad de certificados para comprobar la identidad del editor del software. Este es el comportamiento normal de todos los programas firmados digitalmente en Microsoft Windows.

¿En qué consiste la tecnología Anti-Stealth?

La tecnología Anti-Stealth proporciona un método efectivo de detección de programas peligrosos (rootkits).

Si el sistema recibe el ataque de código malicioso que se comporta como un rootkit, los datos del usuario podrían dañarse o ser robados. Sin una herramienta especial contra programas peligrosos (rootkit), resulta casi imposible detectar programas peligrosos.

¿Por qué a veces hay archivos con la marca "Firmado por MS" que, al mismo tiempo, tienen una entrada de "Nombre de compañía" diferente?

Al intentar identificar la firma digital de un archivo ejecutable, ESET SysInspector comprueba primero si el archivo contiene una firma digital. Si se encuentra una firma digital, se validará el archivo utilizando esa información. Si no se encuentra una firma digital, el ESI comenzará a buscar el archivo CAT correspondiente (Security Catalog - *%systemroot%\system32\catroot*) que contenga información sobre el archivo ejecutable en proceso. Si se encuentra el archivo CAT, la firma digital de dicho archivo se utilizará para el proceso de validación del archivo ejecutable.

Esta es la razón por la que a veces encontramos archivos marcados como "Firmados por MS" pero con un "Nombre de compañía" diferente.

4.7.7.2.6 ESET SysInspector como parte de ESET Mail Security

Para abrir la sección ESET SysInspector en ESET Mail Security, haga clic en **Herramientas** > **ESET SysInspector**. El sistema de administración de la ventana de ESET SysInspector es parecido al de los registros de análisis del ordenador o las tareas programadas. Se puede acceder a todas las operaciones con instantáneas del sistema (como crear, ver, comparar, eliminar y exportar) simplemente haciendo clic una o dos veces.

La ventana de ESET SysInspector contiene información básica acerca de las instantáneas creadas como, por ejemplo, la hora de creación, un breve comentario, el nombre del usuario que ha creado la instantánea y el estado de esta.

Para comparar, crear o eliminar instantáneas, utilice los botones correspondientes ubicados debajo de la lista de instantáneas de la ventana de ESET SysInspector. Estas opciones también están disponibles en el menú contextual. Para ver la instantánea del sistema seleccionada, seleccione **Mostrar** en el menú contextual. Para exportar la instantánea seleccionada a un archivo, haga clic con el botón derecho del ratón en ella y seleccione **Exportar**.

A continuación, se muestra una descripción detallada de las opciones disponibles:

- **Comparar**: le permite comparar dos registros existentes. Esta opción es ideal para realizar un seguimiento de los cambios entre el registro actual y el anterior. Para poder aplicar esta opción, debe seleccionar dos instantáneas con el fin de compararlas.
- **Crear**: crea un registro nuevo. Debe introducir antes un breve comentario acerca del registro. Para ver el progreso de la creación de instantáneas (de la instantánea que se está generando), consulte la columna **Estado**. Todas las instantáneas completadas aparecen marcadas con el estado **Creada**.
- **Eliminar/Eliminar todo**: elimina entradas de la lista.
- **Exportar**: guarda la entrada seleccionada en un archivo XML (y también en una versión comprimida).

4.7.8 ESET SysRescue Live

ESET SysRescue Live es una utilidad que le permite crear un disco de inicio que contenga una de las soluciones de ESET Security, ya sea ESET NOD32 Antivirus, ESET Smart Security o determinados productos diseñados para servidores. La principal ventaja de ESET SysRescue Live es que la solución ESET Security se puede ejecutar de forma independiente del sistema operativo host, pero tiene directo al disco y a todo el sistema de archivos. Gracias a esto, es posible eliminar las amenazas que normalmente no se podrían suprimir como, por ejemplo, cuando el sistema operativo se está ejecutando.

4.7.9 Planificador de tareas

Tareas programadas administra e inicia las tareas programadas con la configuración y las propiedades predefinidas. La configuración y las propiedades contienen información como la fecha y la hora, así como los perfiles que se van a utilizar durante la ejecución de la tarea.

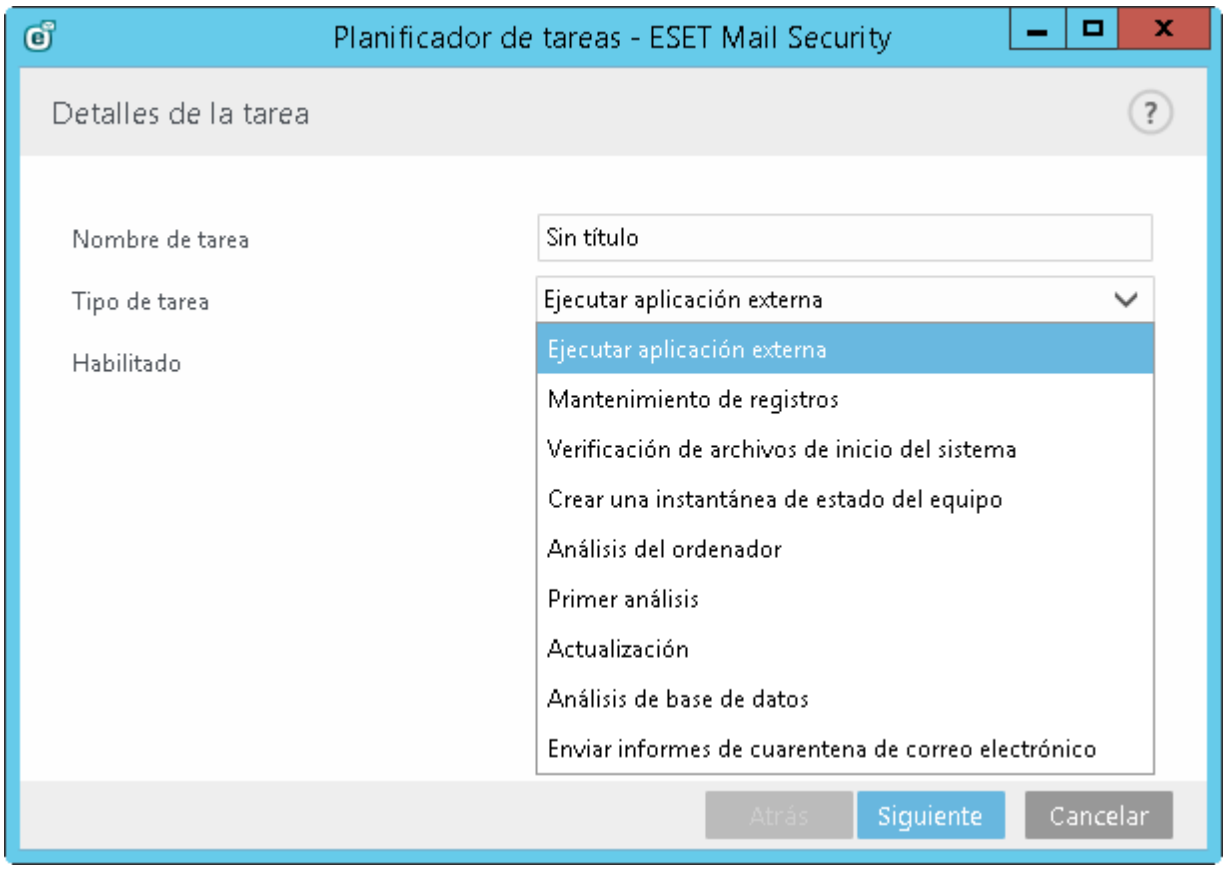
Se puede acceder a Tareas programadas desde la ventana principal del programa de ESET Mail Security; para ello haga clic en **Herramientas** > **Tareas programadas**. **Tareas programadas** contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos utilizados.

Tareas programadas puede utilizarse para programar las siguientes tareas: actualización de base de firmas de virus, análisis de virus, verificación de archivos en el inicio del sistema y mantenimiento de registros. Puede agregar o eliminar tareas directamente desde la ventana Tareas programadas (haga clic en **Agregar tarea** o **Eliminar**). Haga clic con el botón derecho en cualquier parte de la ventana Tareas programadas para realizar las siguientes acciones: mostrar detalles de la tarea, ejecutar la tarea inmediatamente, agregar una tarea nueva y eliminar una tarea existente. Utilice las casillas de verificación disponibles al comienzo de cada entrada para activar o desactivar las tareas.

De forma predeterminada, en **Tareas programadas** se muestran las siguientes tareas programadas:

- **Mantenimiento de registros**
- **Actualización automática de rutina**
- **Actualización automática tras conexión de acceso telefónico**
- **Actualización automática tras el registro del usuario**
- **Verificación automática de los archivos de inicio** (tras inicio de sesión del usuario)
- **Verificación automática de los archivos de inicio** (tras la correcta actualización de la base de firmas de virus)
- **Primer análisis automática**

Para modificar la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario), haga clic con el botón derecho en la tarea y, a continuación, haga clic en **Editar**, o seleccione la tarea que desea modificar y haga clic en **Editar**.



Agregar una nueva tarea

1. Haga clic en **Agregar tarea** en la parte inferior de la ventana.
2. Introduzca un nombre para la tarea.

3. Seleccione la tarea deseada en el menú desplegable:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos de inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear un informe de estado del sistema**: crea una instantánea del ordenador de ESET SysInspector, recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Primer análisis**: de forma predeterminada, 20 minutos después de la instalación o el reinicio se realizará un análisis del ordenador como una tarea de prioridad baja.
- **Actualizar**: programa una tarea de actualización mediante la actualización de la base de firmas de virus y los módulos del programa.
- **Análisis de base de datos**: programa el análisis de la base de datos, puede seleccionar los objetos de análisis (carpetas públicas, bases de datos y buzones) de la misma forma que al configurar el análisis de la base de datos a petición.
- **Enviar informes de cuarentena**: aplicable solamente a Cuarentena local. Envía informes que contienen el estado de la cuarentena y su contenido, incluidos enlaces a la interfaz web de la cuarentena de correo, que le permiten ver y gestionar rápidamente los objetos de correo electrónico que se encuentran en la cuarentena. Puede especificar la dirección de correo electrónico del destinatario de los informes de cuarentena.

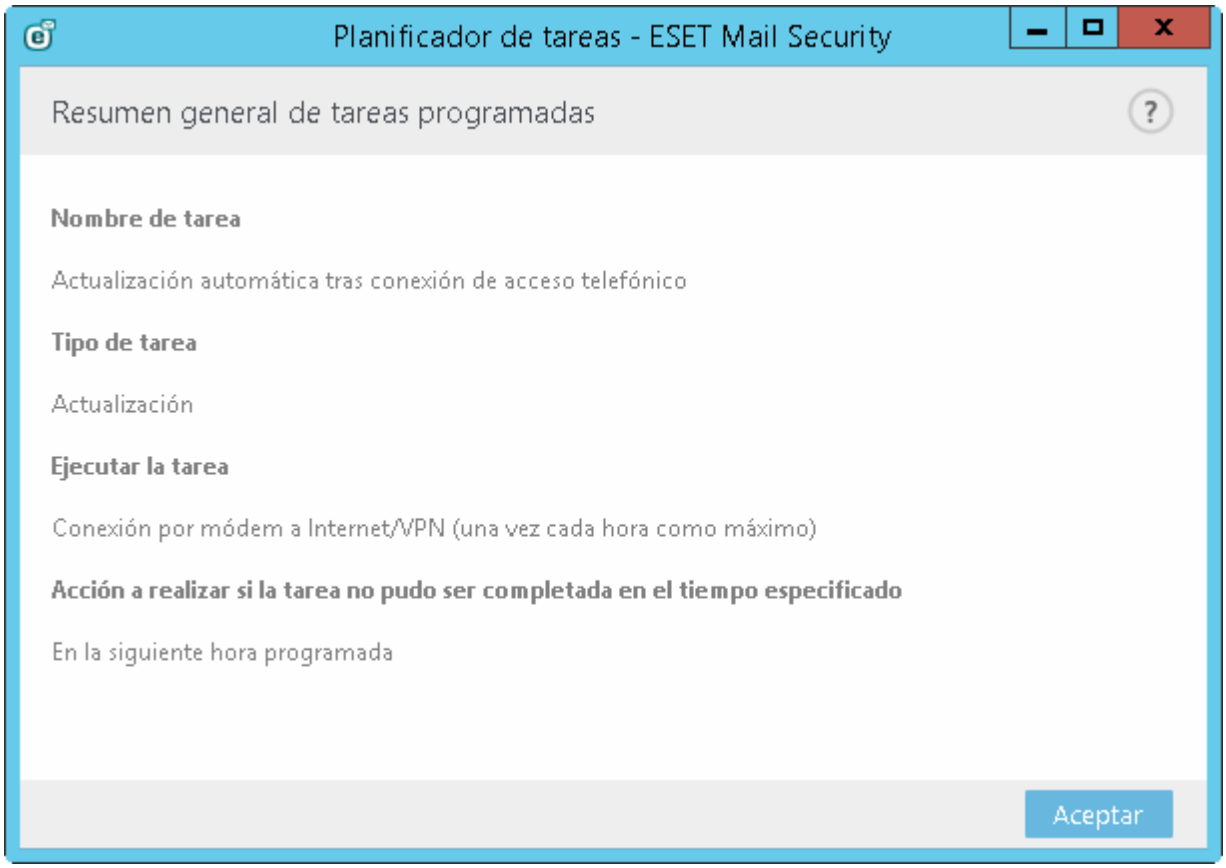
4. Haga clic en el conmutador **Activado** si desea activar la tarea (puede hacerlo más adelante mediante la casilla de verificación situada en la lista de tareas programas), haga clic en **Siguiente** y seleccione una de las opciones de programación:

- **Una vez**: la tarea se ejecutará en la fecha y a la hora predefinidas.
- **Reiteradamente**: la tarea se realizará con el intervalo de tiempo especificado.
- **Diariamente**: la tarea se ejecutará todos los días a la hora especificada.
- **Semanalmente**: la tarea se ejecutará el día y a la hora seleccionados.
- **Desencadenada por un suceso**: la tarea se ejecutará tras un suceso especificado.

5. Seleccione **No ejecutar la tarea si está funcionando con batería** para minimizar los recursos del sistema mientras un ordenador portátil esté funcionando con batería. La tarea se ejecutará en la fecha y hora especificadas en el campo **Ejecución de la tarea**. Si la tarea no se pudo ejecutar en el tiempo predefinido, puede especificar cuándo se ejecutará de nuevo:

- **En la siguiente hora programada**
- **Lo antes posible**
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el cuadro **Tiempo desde la última ejecución**)

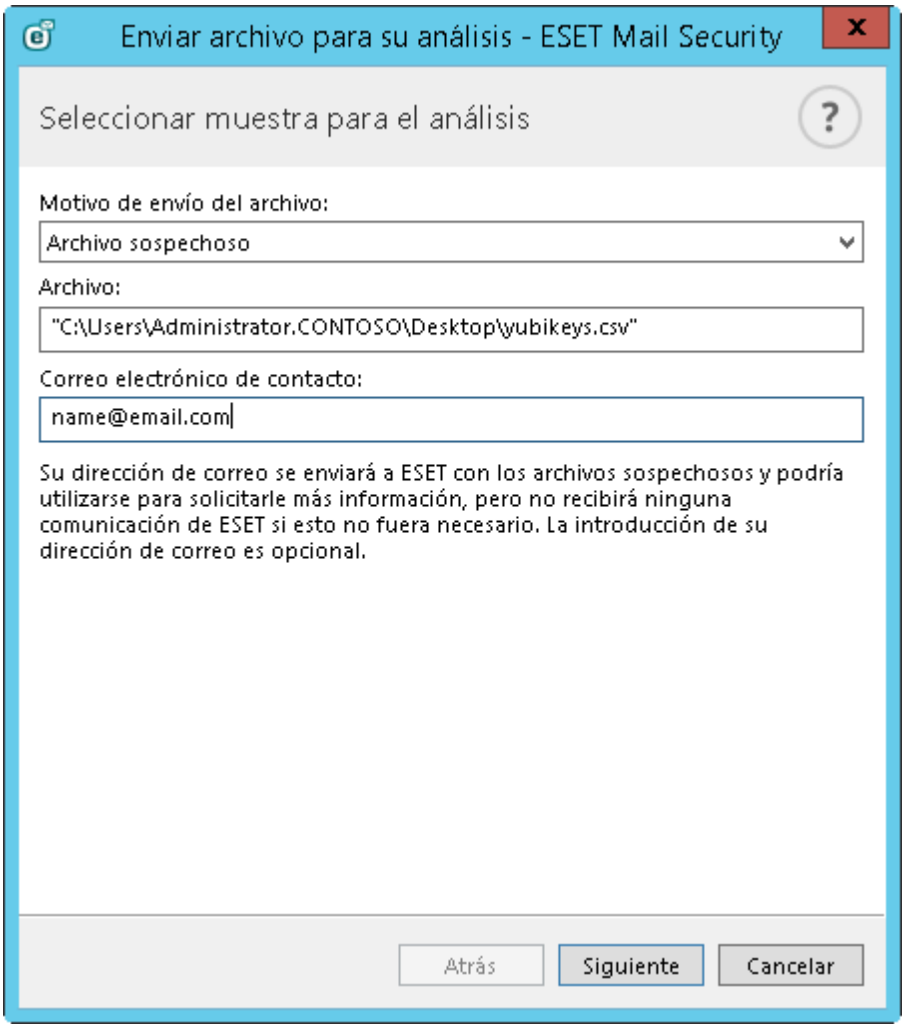
Haga clic con el botón derecho del ratón en una tarea y, a continuación, en **Mostrar detalles de la tarea** en el menú contextual para consultar información sobre la tarea.


Planificador de tareas - ESET Mail Security
Resumen general de tareas programadas
Nombre de tarea
Actualización automática tras conexión de acceso telefónico
Tipo de tarea
Actualización
Ejecutar la tarea
Conexión por módem a Internet/VPN (una vez cada hora como máximo)
Acción a realizar si la tarea no pudo ser completada en el tiempo especificado
En la siguiente hora programada
Aceptar

4.7.10 Enviar muestras para su análisis

El cuadro de diálogo de envío de muestras le permite enviar un archivo o un sitio a ESET para que lo analice; esta opción está disponible en **Herramientas** > **Enviar muestra para su análisis**. Si encuentra un archivo en su ordenador que se comporta de manera sospechosa o un sitio sospechoso en Internet, puede enviarlo al laboratorio de virus de ESET para su análisis. Si resulta que el archivo es una aplicación o un sitio web malicioso, su detección se agregará a una actualización futura.

También puede enviar el archivo por correo electrónico. Para ello, comprima los archivos con un programa como WinRAR o WinZip, proteja el archivo comprimido con la contraseña "infected" y envíelo a samples@eset.com. Utilice un asunto descriptivo y adjunte toda la información posible sobre el archivo (por ejemplo, el sitio web del que lo descargó).


Enviar archivo para su análisis - ESET Mail Security
Seleccionar muestra para el análisis
Motivo de envío del archivo:
Archivo sospechoso
Archivo:
"C:\Users\Administrator.CONTOSO\Desktop\yubikeys.csv"
Correo electrónico de contacto:
name@email.com
Su dirección de correo se enviará a ESET con los archivos sospechosos y podría utilizarse para solicitarle más información, pero no recibirá ninguna comunicación de ESET si esto no fuera necesario. La introducción de su dirección de correo es opcional.
Atrás
Siguiente
Cancelar

NOTA: Antes de enviar una muestra a ESET, asegúrese de que cumple uno o más de los siguientes criterios:

- El archivo o sitio web no se detecta en absoluto.
- El archivo o sitio web se detecta como una amenaza, pero no lo es.

No recibirá ninguna respuesta a menos que se requiera información adicional para poder realizar el análisis.

Seleccione la descripción en el menú desplegable **Motivo de envío de la muestra** que mejor se ajuste a su mensaje:

- **Archivo sospechoso**
- **Sitio web sospechoso** (sitio web que está infectado por código malicioso)
- **Archivo de falso positivo** (archivo que se detecta como amenaza pero no está infectado)
- **Sitio de falso positivo**
- **Otros**

Archivo/Sitio: la ruta del archivo o sitio web que quiere enviar.

Correo electrónico de contacto: la dirección de correo de contacto se envía a ESET junto con los archivos sospechosos, y se puede utilizar para ponernos en contacto con usted en caso de que sea necesario enviar más información para poder realizar el análisis. No es obligatorio introducir una dirección de correo electrónico de contacto. No obtendrá ninguna respuesta de ESET a menos que sea necesario enviar información adicional, ya que cada día nuestros servidores reciben decenas de miles de archivos, lo que hace imposible responder a todos los envíos.

4.7.10.1 Archivo sospechoso

Signos y síntomas observados de la infección por código malicioso: describa el comportamiento del archivo sospechoso que ha observado en el ordenador.

Origen del archivo (dirección URL o proveedor): escriba el origen (fuente) del archivo y cómo llegó a él.

Notas e información adicional: aquí puede especificar más información o una descripción que le ayude con el proceso de identificación del archivo sospechoso.

NOTA: El primer parámetro (**Signos y síntomas observados de la infección por código malicioso**) es necesario; la información adicional que proporcione será de gran utilidad para nuestros laboratorios en el proceso de identificación de muestras.

4.7.10.2 Sitio web sospechoso

Seleccione una de las opciones siguientes en el menú desplegable **Problema del sitio**:

- **Infectado**: sitio web que contiene virus u otro código malicioso distribuido por diversos métodos.
- **Phishing**: su objetivo suele ser acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc. Puede obtener más información sobre este tipo de ataque en el glosario.
- **Fraude**: un sitio web fraudulento o de estafas.
- Seleccione **Otros** si las opciones anteriores no hacen referencia al sitio que va a enviar.

Notas e información adicional: aquí puede especificar más información o una descripción que ayude a analizar el sitio web sospechoso.

4.7.10.3 Archivo de falso positivo

Le rogamos que nos envíe los archivos que se detectan como amenazas pero no están infectados para mejorar nuestro motor de antivirus y antiespía y ayudar a proteger a otras personas. Los falsos positivos (FP) se generan cuando el patrón de un archivo coincide con un mismo patrón disponible en una base de firmas de virus.

Nombre y versión de la aplicación: título y versión del programa (por ejemplo, número, alias o nombre en código).

Origen del archivo (dirección URL o proveedor): escriba el origen (fuente) del archivo y cómo llego a él.

Objetivo de la aplicación: descripción general de la aplicación, tipo de aplicación (por ejemplo, navegador, reproductor multimedia, etc.) y su funcionalidad.

Notas e información adicional: aquí puede especificar más información o una descripción que ayude a procesar el archivo sospechoso.

NOTA: los tres primeros parámetros son necesarios para identificar las aplicaciones legítimas y distinguirlas del código malicioso. La información adicional que proporcione será de gran ayuda para los procesos de identificación y procesamiento de muestras en nuestros laboratorios.

4.7.10.4 Sitio de falso positivo

Le rogamos que nos envíe los sitios que se detectan como amenazas, fraudes o phishing, pero no lo son. Los falsos positivos (FP) se generan cuando el patrón de un archivo coincide con un mismo patrón disponible en una base de firmas de virus. Proporcione este sitio web para mejorar nuestro motor de antivirus y anti-phishing y ayudar a proteger a otras personas.

Notas e información adicional: aquí puede especificar más información o una descripción que ayude a procesar el archivo sospechoso.

4.7.10.5 Otros

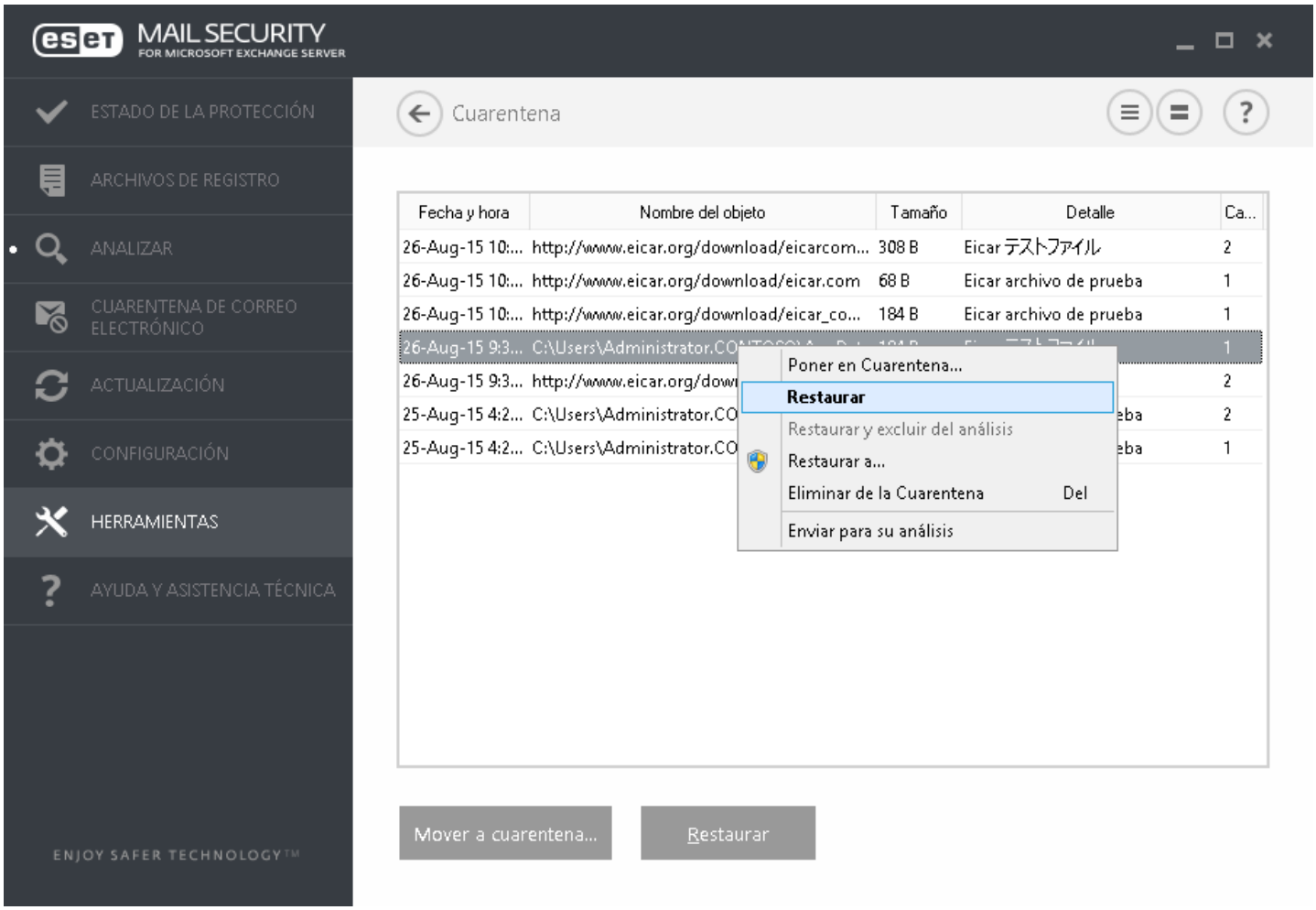
Utilice este formulario si el archivo no se puede categorizar como un **Archivo sospechoso** o un **Falso positivo**.

Motivo de envío del archivo: introduzca una descripción detallada y el motivo por el que envía el archivo.

4.7.11 Cuarentena

La función principal de la cuarentena es almacenar los archivos infectados de forma segura. Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si ESET Mail Security los detecta incorrectamente como infectados.

Es posible poner en cuarentena cualquier archivo. La cuarentena se recomienda cuando el comportamiento de un archivo es sospechoso y el análisis no lo ha detectado. Los archivos en cuarentena se pueden enviar para su análisis al laboratorio de virus de ESET.



Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra la fecha y la hora en que se pusieron en cuarentena, la ruta de la ubicación original del archivo infectado, su tamaño en bytes, el motivo (agregado por el usuario, por ejemplo) y el número de amenazas (por ejemplo, si se trata de un archivo comprimido que contiene varias amenazas).

En el caso de que los objetos del mensaje de correo electrónico se pongan en cuarentena en la cuarentena de archivos, se mostrará información en forma de ruta al buzón de correo, la carpeta o el nombre del archivo.

Puesta de archivos en cuarentena

ESET Mail Security pone los archivos eliminados en cuarentena automáticamente (si no ha desactivado esta opción en la ventana de alerta). Si lo desea, puede copiar en cuarentena cualquier archivo sospechoso de forma manual, haciendo clic en el botón **Poner en cuarentena.** Los archivos que se pongan en cuarentena se quitarán de su ubicación original. El menú contextual también se puede utilizar con este fin: haga clic con el botón derecho en la ventana **Cuarentena** y seleccione **Poner en cuarentena**.

Restauración de archivos de cuarentena

Los archivos puestos en cuarentena se pueden restaurar a su ubicación original. Para ello, utilice la función **Restaurar**, disponible en el menú contextual que se abre al hacer clic con el botón derecho del ratón en la ventana Cuarentena. Si el archivo está marcado como aplicación potencialmente no deseada, también estará disponible la opción **Restaurar y excluir del análisis**. Puede obtener más información sobre este tipo de aplicación en el glosario. El menú contextual también ofrece la opción **Restaurar a...**, que le permite restaurar archivos en una ubicación distinta a la original de la cual se eliminaron.

NOTA: si el programa ha puesto en cuarentena un archivo no dañino por error, exclúyalo del análisis después de restaurarlo y enviarlo al servicio de atención al cliente de ESET.

Envío de un archivo de cuarentena

Si ha copiado en cuarentena un archivo sospechoso que el programa no ha detectado o si se ha determinado incorrectamente que un archivo está infectado (por ejemplo, por el análisis heurístico del código) y, consecuentemente, se ha copiado a cuarentena, envíe el archivo al laboratorio de virus de ESET. Para enviar un archivo de cuarentena, haga clic con el botón derecho del ratón en el archivo y seleccione **Enviar para su análisis** en el menú contextual.

4.8 Ayuda y asistencia técnica

ESET Mail Security contiene herramientas de resolución de problemas e información de soporte que le ayudará a solucionar los problemas que se encuentre.

Ayuda

- **Buscar en la base de conocimientos de ESET**: la base de conocimiento de ESET contiene respuestas a las preguntas más frecuentes y posibles soluciones a diferentes problemas. La actualización periódica por parte de los especialistas técnicos de ESET convierte esta base de conocimiento en la herramienta más potente para resolver diversos problemas.
- **Abrir la ayuda**: haga clic en este enlace para abrir las páginas de ayuda de ESET Mail Security.
- **Encontrar una solución rápida**: seleccione esta opción para buscar soluciones a los problemas más frecuentes. Es recomendable que lea atentamente esta sección antes de ponerse en contacto con el equipo de asistencia técnica.

Servicio de atención al cliente

- **Enviar una solicitud de soporte**: si no encuentra respuesta a su problema, también puede usar este formulario del sitio web de ESET para ponerse rápidamente en contacto con nuestro departamento de atención al cliente.

Herramientas de soporte

- **Enciclopedia de amenazas**: es un enlace a la enciclopedia de amenazas de ESET, que contiene información sobre los peligros y los síntomas de diferentes tipos de amenaza.
- **Historial de la base de firmas de virus**: proporciona un enlace al radar de virus de ESET, que contiene información sobre las versiones de la base de firmas de virus de ESET.
- **Limpiador especializado ESET**: esta aplicación de desinfección identifica y elimina automáticamente infecciones por código malicioso comunes; para obtener más información, visite este artículo de la base de conocimiento de ESET.

Información del producto y la licencia

- **Acerca de ESET Mail Security**: muestra información sobre su copia de ESET Mail Security.
- Administrar licencia: haga clic para abrir la ventana de activación del producto. Seleccione uno de los métodos disponibles para activar ESET Mail Security. Consulte Cómo activar ESET Mail Security para obtener más información.

4.8.1 Cómo

Este capítulo abarca algunas de las preguntas más frecuentes y los problemas encontrados. Haga clic en el título del tema para obtener información sobre cómo solucionar el problema:

Cómo actualizar ESET Mail Security

Cómo activar ESET Mail Security

Cómo programar una tarea de análisis (cada 24 horas)

Cómo eliminar un virus del servidor

Cómo funcionan las exclusiones automáticas

Si no encuentra su problema en las páginas de ayuda anteriores, utilice una palabra clave o frase que describa el problema para realizar la búsqueda en las páginas de ayuda de ESET Mail Security.

Si no encuentra la solución a su problema o consulta en las páginas de ayuda, puede probar con nuestra base de datos de conocimiento en línea, que se actualiza periódicamente.

Si es necesario, puede ponerse en contacto directamente con nuestro centro de soporte técnico en línea para comunicarle sus consultas o problemas. Puede acceder al formulario de contacto desde la ficha Ayuda y asistencia técnica del programa de ESET.

4.8.1.1 Cómo actualizar ESET Mail Security

ESET Mail Security se puede actualizar de forma manual o automática. Para activar la actualización, haga clic en **Actualizar la base de firmas de virus ahora**, que encontrará en la sección **Actualización** del programa.

Los parámetros de instalación predeterminados crean una tarea de actualización automática que se lleva a cabo cada hora. Si tiene que cambiar el intervalo, vaya a **Tareas programadas** (para obtener más información sobre Tareas programadas, haga clic aquí).

4.8.1.2 Cómo activar ESET Mail Security

Cuando haya finalizado la instalación, se le solicitará que active el producto.

Hay varios métodos de activar su producto. La disponibilidad de un método concreto de activación en la ventana de activación puede variar en función del país, además de los medios de distribución (CD/DVD, página web de ESET, etc.).

Para activar su copia de ESET Mail Security directamente desde el programa, haga clic en el icono de la bandeja del sistema y seleccione **Activar licencia del producto** en el menú. El producto también se puede activar desde el menú principal, en **Ayuda y asistencia técnica** > **Activar licencia** o **Estado de la protección** > **Activar licencia del producto**.

Puede utilizar cualquiera de estos métodos para activar ESET Mail Security:

- **Clave de licencia**: se trata de una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX y sirve para identificar al propietario de la licencia y activar la licencia.
- **Cuenta del administrador de seguridad**: es una cuenta creada en el portal del administrador de licencias de ESET con credenciales (dirección de correo electrónico y contraseña). Este método le permite gestionar varias licencias desde una ubicación.
- **Archivo de licencia sin conexión**: se trata de un archivo generado automáticamente que se transferirá al producto de ESET para proporcionar información sobre la licencia. El archivo de licencia sin conexión se genera en el portal de licencias y se utiliza en aquellos entornos en los que la aplicación no se puede conectar a la autoridad de concesión de licencias.

Haga clic en **Activar más tarde** con ESET Remote Administrator si su ordenador forma parte de una red administrada y el administrador realizará la activación remota a través de ESET Remote Administrator. También puede usar esta opción si desea activar el cliente más adelante.

Haga clic en **Ayuda y asistencia técnica** > **Administrar licencia** en la ventana principal del programa para administrar la información de su licencia cuando desee. Verá el ID de la licencia pública utilizado para que ESET identifique su producto y para la identificación de la licencia. El nombre de usuario con el que se ha registrado el ordenador en el sistema de licencias se almacena en la sección **Acerca de**; esta puede mostrarse al hacer clic con el botón derecho del ratón en el icono de la bandeja del sistema .

NOTA: ESET Remote Administrator puede activar ordenadores cliente de forma silenciosa con las licencias que le proporcione el administrador.

4.8.1.3 Cómo cuenta ESET Mail Security los buzones de correo

Para obtener más información, consulte el artículo de nuestra base de conocimiento.

4.8.1.4 Cómo crear una tarea nueva en Tareas programadas

Para crear una tarea nueva en **Herramientas** > **Tareas programadas**, haga clic en **Agregar tarea** o haga clic con el botón derecho y seleccione **Agregar** en el menú contextual. Están disponibles cinco tipos de tareas programadas:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador**: analiza los archivos y las carpetas del ordenador.
- **Primer análisis**: de forma predeterminada, 20 minutos después de la instalación o el reinicio se realizará un análisis del ordenador como una tarea de prioridad baja.
- **Actualizar**: programa una tarea de actualización mediante la actualización de la base de firmas de virus y los módulos del programa.

La **Actualización** es una de las tareas programadas más frecuentes, por lo que a continuación explicaremos cómo se agrega una nueva tarea de actualización:

En el menú desplegable **Tarea programada**, seleccione **Actualización**. Introduzca el nombre de la tarea en el campo **Nombre de la tarea** y haga clic en **Siguiente**. Seleccione la frecuencia de la tarea. Están disponibles las opciones siguientes: **Una vez**, **Reiteradamente**, **Diariamente**, **Semanalmente** y **Cuando se cumpla la condición.** Seleccione **No ejecutar la tarea si está funcionando con batería** para minimizar los recursos del sistema mientras un ordenador portátil esté funcionando con batería. La tarea se ejecutará en la fecha y hora especificadas en el campo **Ejecución de la tarea**. A continuación, defina la acción que debe llevarse a cabo si la tarea no se puede realizar o completar a la hora programada. Están disponibles las opciones siguientes:

- **En la siguiente hora programada**
- **Lo antes posible**
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el cuadro Tiempo desde la última ejecución)

En el paso siguiente se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente. Haga clic en **Finalizar** cuando haya terminado de hacer cambios.

Aparecerá un cuadro de diálogo que permite al usuario elegir los perfiles que desea utilizar para la tarea programada. Aquí puede definir los perfiles principal y alternativo. El perfil alternativo se utiliza cuando la tarea no se puede completar con el perfil principal. Haga clic en **Finalizar** para confirmar la operación; la nueva tarea se agregará a la lista de tareas programadas actualmente.

4.8.1.5 Cómo programar una tarea de análisis (cada 24 horas)

Para programar una tarea periódica, diríjase a **ESET Mail Security** > **Herramientas** > **Tareas programadas**. A continuación se indican las instrucciones básicas para programar una tarea que analice los discos locales cada 24 horas.

Para programar una tarea:

1. Haga clic en **Agregar** en la pantalla principal de Tareas programadas.
2. Seleccione **Análisis del ordenador a petición** en el menú desplegable.
3. Escriba un nombre para la tarea y seleccione **Reiteradamente**.
4. Seleccione la opción para ejecutar la tarea cada 24 horas (1440 minutos).
5. Seleccione la acción que debe realizarse si se produce un error al ejecutar la tarea programada por cualquier motivo.
6. Revise el resumen de la tarea programada y haga clic en **Finalizar**.
7. En el menú desplegable **Objetos**, seleccione Discos locales.
8. Haga clic en **Finalizar** para aplicar la tarea.

4.8.1.6 Cómo eliminar un virus del servidor

Si su ordenador muestra señales de una infección por código malicioso, por ejemplo, es más lento o se bloquea a menudo, se recomienda que haga lo siguiente:

1. En la ventana principal de ESET Mail Security, haga clic en **Análisis del ordenador**.
2. Haga clic en **Análisis estándar** para iniciar el análisis del sistema.
3. Una vez finalizado el análisis, revise el registro con el número de archivos analizados, infectados y desinfectados.
4. Si solo desea analizar determinadas partes del disco, seleccione la opción **Análisis personalizado** y especifique los objetos que desee analizar en busca de virus.

4.8.2 Enviar una solicitud de soporte

Con el fin de prestar asistencia con la máxima rapidez y precisión posibles, ESET requiere información sobre la configuración de ESET Mail Security, información detallada del sistema y de los procesos en ejecución (Archivo de registro de ESET SysInspector), así como datos del registro. ESET utilizará estos datos solo para prestar asistencia técnica al cliente.

Al enviar el formulario web a ESET también se enviarán los datos de configuración de su sistema. Seleccione **Enviar siempre esta información** si desea recordar esta acción para este proceso. Si desea enviar el formulario sin datos, haga clic en **No enviar datos** y podrá ponerse en contacto con el servicio de atención al cliente de ESET mediante el formulario de asistencia a través de Internet.

Este ajuste también puede configurarse en **Configuración avanzada** > **Herramientas** > **Diagnósticos** > **Atención al cliente**.

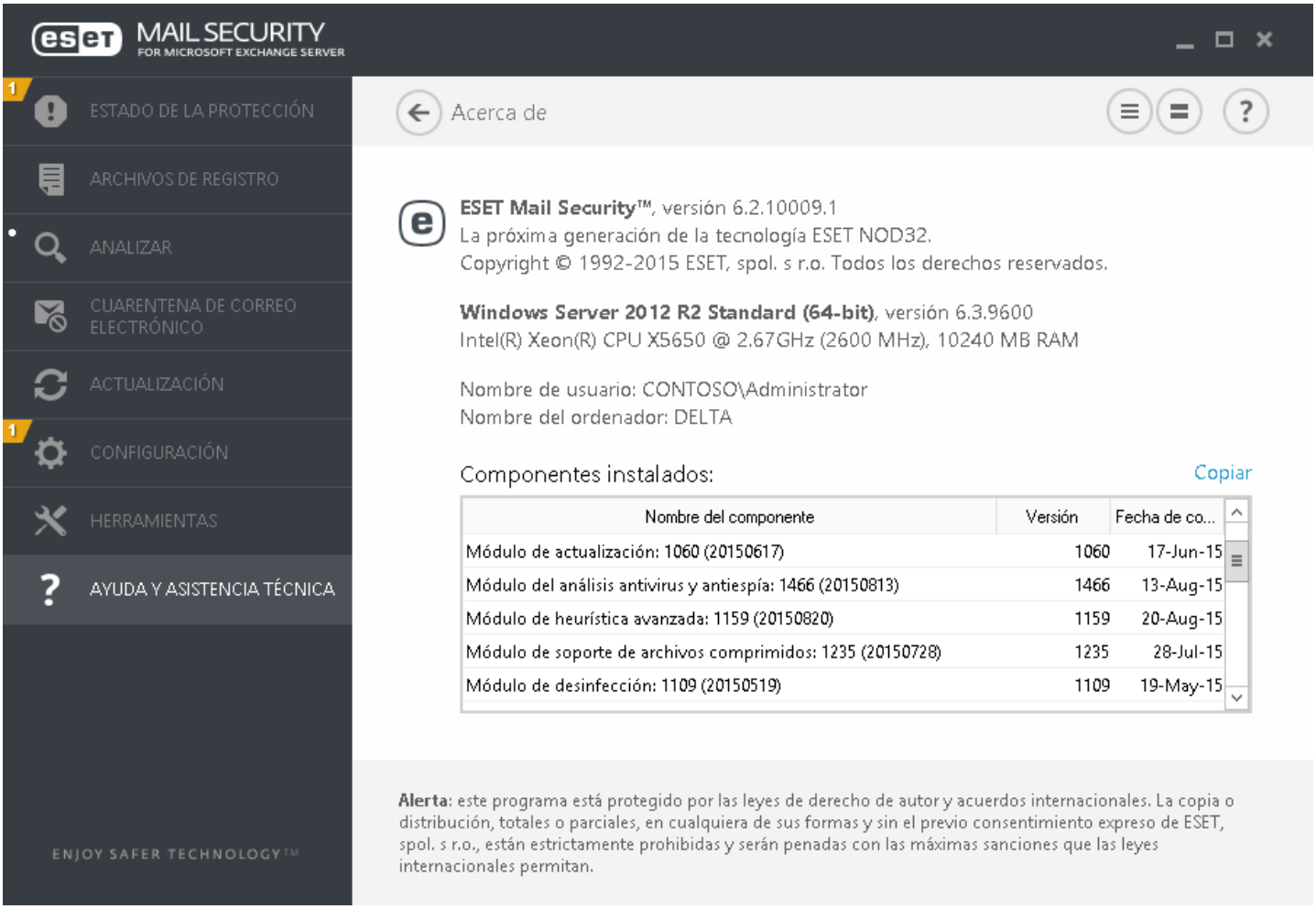
NOTA: si ha optado por enviar los datos del sistema, es necesario cumplimentar y enviar el formulario web o, de lo contrario, no se creará su parte y se perderán los datos de su sistema.

4.8.3 Limpiador especializado ESET

El Limpiador especializado ESET es una herramienta de eliminación para infecciones comunes por código malicioso, como Conficker, Sirefef o Necurs. Consulte este artículo de la base de conocimiento de ESET para obtener más información.

4.8.4 Acerca de ESET Mail Security

Esta ventana contiene información sobre la versión instalada de ESET Mail Security y la lista de módulos de programa instalados. En la parte superior de la ventana se muestra información sobre el sistema operativo y los recursos del sistema.


MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
ESTADO DE LA PROTECCIÓN
ARCHIVOS DE REGISTRO
ANALIZAR
CUARENTENA DE CORREO ELECTRÓNICO
ACTUALIZACIÓN
CONFIGURACIÓN
HERRAMIENTAS
AYUDA Y ASISTENCIA TÉCNICA
ENJOY SAFER TECHNOLOGY™
Acerca de
ESET Mail Security™, versión 6.2.10009.1
La próxima generación de la tecnología ESET NOD32.
Copyright © 1992-2015 ESET, spol. s r.o. Todos los derechos reservados.
Windows Server 2012 R2 Standard (64-bit), versión 6.3.9600
Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (2600 MHz), 10240 MB RAM
Nombre de usuario: CONTOSO\Administrator
Nombre del ordenador: DELTA
Componentes instalados:
Copiar
Nombre del componente
Versión
Fecha de co...
Módulo de actualización: 1060 (20150617) 1060 17-Jun-15
Módulo del análisis antivirus y antiespía: 1466 (20150813) 1466 13-Aug-15
Módulo de heurística avanzada: 1159 (20150820) 1159 20-Aug-15
Módulo de soporte de archivos comprimidos: 1235 (20150728) 1235 28-Jul-15
Módulo de desinfección: 1109 (20150519) 1109 19-May-15
Alerta: este programa está protegido por las leyes de derecho de autor y acuerdos internacionales. La copia o distribución, totales o parciales, en cualquiera de sus formas y sin el previo consentimiento expreso de ESET, spol. s r.o., están estrictamente prohibidas y serán penadas con las máximas sanciones que las leyes internacionales permitan.

Puede copiar al portapapeles la información de los módulos (**Componentes instalados**) haciendo clic en **Copiar**. Esta información puede resultarle de utilidad durante la resolución de problemas o cuando se ponga en contacto con el servicio de asistencia técnica.

4.8.5 Activación del producto

Cuando haya finalizado la instalación, se le solicitará que active el producto.

Hay varios métodos de activar su producto. La disponibilidad de un método concreto de activación en la ventana de activación puede variar en función del país, además de los medios de distribución (CD/DVD, página web de ESET, etc.).

Para activar su copia de ESET Mail Security directamente desde el programa, haga clic en el icono de la bandeja del sistema y seleccione **Activar licencia del producto** en el menú. El producto también se puede activar desde el menú principal, en **Ayuda y asistencia técnica** > **Activar licencia** o **Estado de la protección** > **Activar licencia del producto**.

Puede utilizar cualquiera de estos métodos para activar ESET Mail Security:

- **Clave de licencia**: se trata de una cadena única que presenta el formato XXXX-XXXX-XXXX-XXXX-XXXX y sirve para identificar al propietario de la licencia y activar la licencia.
- **Cuenta del administrador de seguridad**: es una cuenta creada en el portal del administrador de licencias de ESET con credenciales (dirección de correo electrónico y contraseña). Este método le permite gestionar varias licencias desde una ubicación.
- **Archivo de licencia sin conexión**: se trata de un archivo generado automáticamente que se transferirá al producto de ESET para proporcionar información sobre la licencia. El archivo de licencia sin conexión se genera en el portal de licencias y se utiliza en aquellos entornos en los que la aplicación no se puede conectar a la autoridad de concesión de licencias.

Haga clic en **Activar más tarde** con ESET Remote Administrator si su ordenador forma parte de una red administrada y el administrador realizará la activación remota a través de ESET Remote Administrator. También puede usar esta opción si desea activar el cliente más adelante.

Haga clic en **Ayuda y asistencia técnica** > **Administrar licencia** en la ventana principal del programa para administrar la información de su licencia cuando desee. Verá el ID de la licencia pública utilizado para que ESET identifique su producto y para la identificación de la licencia. El nombre de usuario con el que se ha registrado el ordenador en el sistema de licencias se almacena en la sección **Acerca de**; esta puede mostrarse al hacer clic con el botón derecho del ratón en el icono de la bandeja del sistema .

NOTA: ESET Remote Administrator puede activar ordenadores cliente de forma silenciosa con las licencias que le proporcione el administrador.

4.8.5.1 Registro

Rellene los campos del formulario de registro y haga clic en **Continuar** para registrar su licencia. Los campos marcados entre paréntesis son obligatorios. La información se utilizará exclusivamente para cuestiones relacionadas con su licencia de ESET.

4.8.5.2 Activación de Administrador de seguridad

La cuenta del administrador de seguridad es una cuenta creada en el portal de licencias con su **dirección de correo electrónico** y su **contraseña**; con esta cuenta se pueden ver todas las autorizaciones de la licencia.

Una cuenta del **administrador de seguridad** le permite gestionar varias licencias. Si no tiene una cuenta de administrador de seguridad, haga clic en **Crear cuenta**; se abrirá la página web del administrador de licencias de ESET, donde se puede registrar con sus credenciales.

Si ha olvidado su contraseña, haga clic en **¿Ha olvidado su contraseña?** para acceder al portal profesional de ESET. Introduzca su dirección de correo electrónico y haga clic en **Enviar** para confirmar. A continuación recibirá un mensaje con instrucciones para restablecer la contraseña.

NOTA: si desea obtener más información sobre el uso de ESET License Administrator, consulte el manual de usuario de ESET License Administrator.

4.8.5.3 Error de activación

ESET Mail Security no se ha activado correctamente. Asegúrese de que ha introducido la **Clave de licencia** adecuada o adjuntado una **Licencia sin conexión**. Si dispone de otra **licencia sin conexión**, vuelva a introducirla. Para revisar la clave de licencia introducida, haga clic en **Comprobar la clave de licencia de nuevo** o en **Comprar una licencia nueva** y se le redirigirá a nuestra web, en la que podrá adquirir una licencia nueva.

4.8.5.4 Licencia

Si selecciona la opción de activación de Administrador de seguridad, se le solicitará que seleccione una licencia asociada a su cuenta para su uso con ESET Mail Security. Haga clic en **Activar** para continuar.

4.8.5.5 Progreso de la activación

ESET Mail Security se está activando. Espere. Esta operación puede tardar un rato.

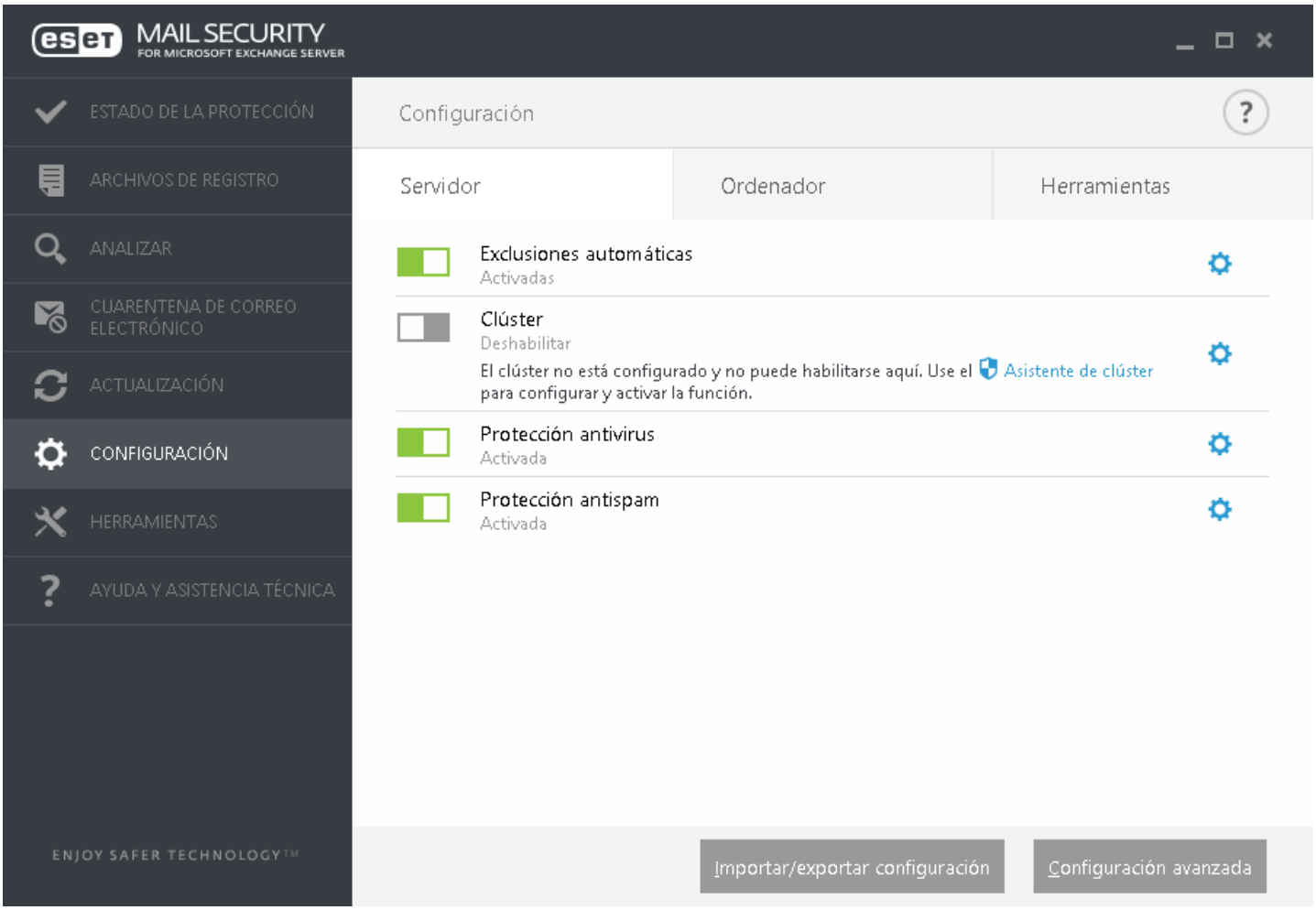
4.8.5.6 La activación se ha realizado correctamente

ESET Mail Security se ha activado correctamente. A partir de ahora, ESET Mail Security recibirá actualizaciones periódicas para identificar las amenazas más recientes y proteger su ordenador. Haga clic en **Listo** para finalizar la activación del producto.

5. Trabajo con ESET Mail Security

El menú **Configuración** contiene las siguientes secciones, entre las que puede cambiar por medio de fichas:

- Servidor
- Ordenador
- Herramientas



Si desea desactivar temporalmente un módulo concreto, haga clic en el conmutador verde situado junto al módulo deseado. Tenga en cuenta que esto puede disminuir el nivel de protección del ordenador.
Para volver a activar la protección de un componente de seguridad desactivado, haga clic en el conmutador rojo .
Para acceder a la configuración detallada de un componente de seguridad determinado, haga clic en la rueda dentada .

Haga clic en **Configuración avanzada** o pulse **F5** para acceder a configuraciones y opciones adicionales del componente.

En la parte inferior de la ventana de configuración encontrará opciones adicionales. Para cargar los parámetros de configuración con un archivo de configuración *.xml*, o para guardar los parámetros de configuración actuales en un archivo de configuración, utilice la opción **Importar/exportar configuración**. Consulte Importar/exportar configuración para obtener más información detallada.

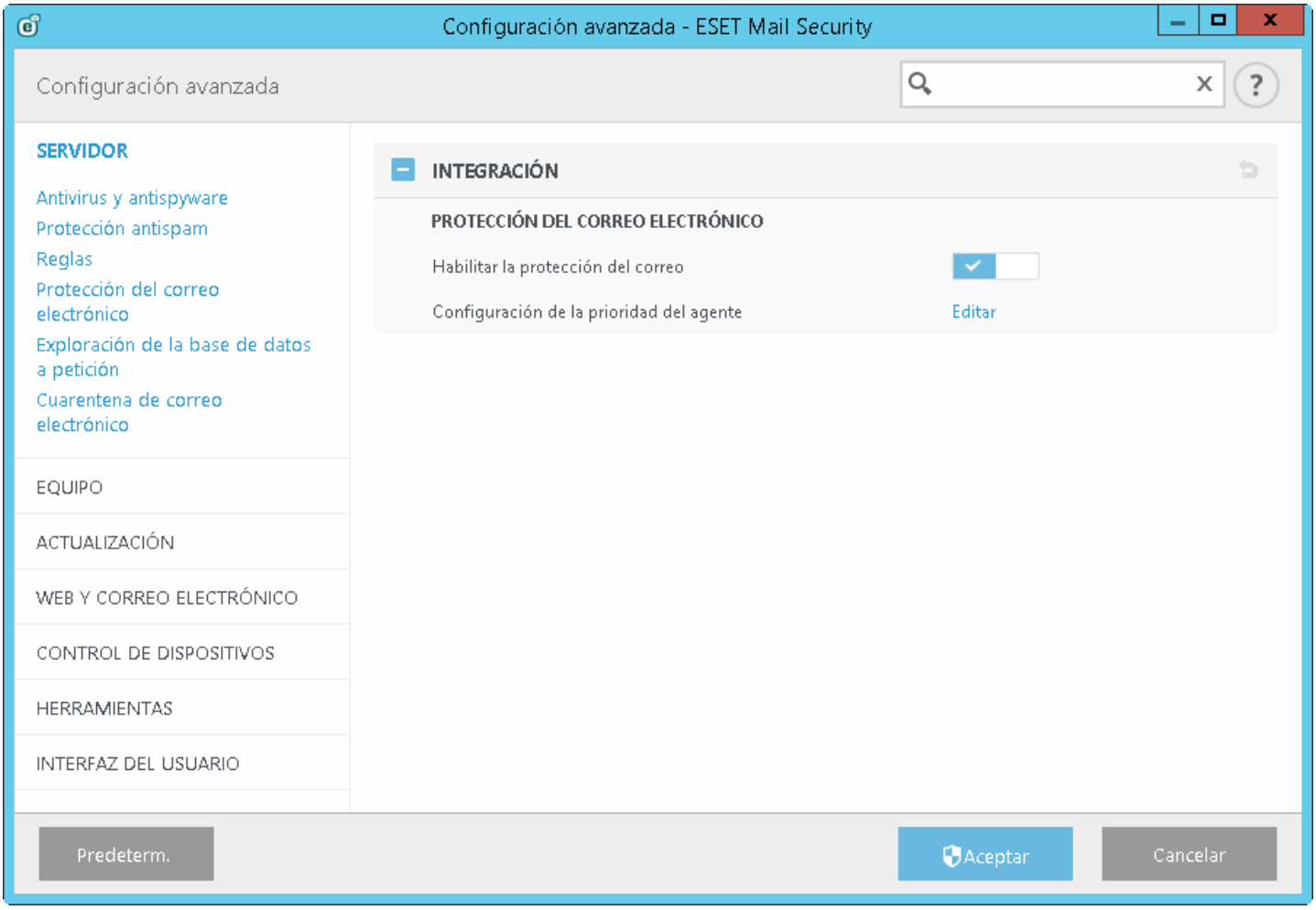
5.1 Servidor

ESET Mail Security proporciona una buena protección para Microsoft Exchange Server por medio de las siguientes funciones:

- Antivirus y antiespía
- Protección antispam
- Reglas
- Protección del correo electrónico (Exchange Server 2007, 2010, 2013)
- Protección de la base de datos de buzones (Exchange Server 2003, 2007, 2010)
- Análisis de la base de datos a petición (Exchange Server 2007, 2010, 2013)
- Cuarentena (configuración del tipo de cuarentena de correo electrónico)

Esta sección de Configuración avanzada le permite activar o desactivar la integración de la Protección de la base de datos de buzones y la Protección del correo electrónico, así como editar la Prioridad del agente.

NOTA: si está ejecutando Microsoft Exchange Server 2007 o 2010, puede optar entre Protección de la base de datos de buzones y Análisis de la base de datos a petición. Sin embargo, solo uno de estos dos tipos de protección puede estar activo al mismo tiempo. Si opta por usar el Análisis de la base de datos a petición, tendrá que desactivar la integración de la Protección de la base de datos de buzones. De lo contrario, el Análisis de la base de datos a petición no estará disponible.



5.1.1 Configuración de prioridad de agentes

En el menú **Configuración de prioridad de agentes** puede definir la prioridad con la que los agentes de ESET Mail Security pasan a ser activos después del inicio del servidor de Microsoft Exchange. El valor numérico define la prioridad. Cuanto más bajo es el número, más alta es la prioridad. Esto es así en Microsoft Exchange 2003.

Si pulsa el botón **Editar** para acceder a la Configuración de prioridad de agentes, podrá definir la prioridad de activación de los agentes de ESET Mail Security cuando Microsoft Exchange Server se haya iniciado.

- **Modificar**: defina este número manualmente para cambiar la prioridad de un agente seleccionado.
- **Subir**: suba la posición de un agente seleccionado en la lista de agentes para aumentar su prioridad.
- **Bajar**: baje la posición de un agente seleccionado en la lista de agentes para reducir su prioridad.

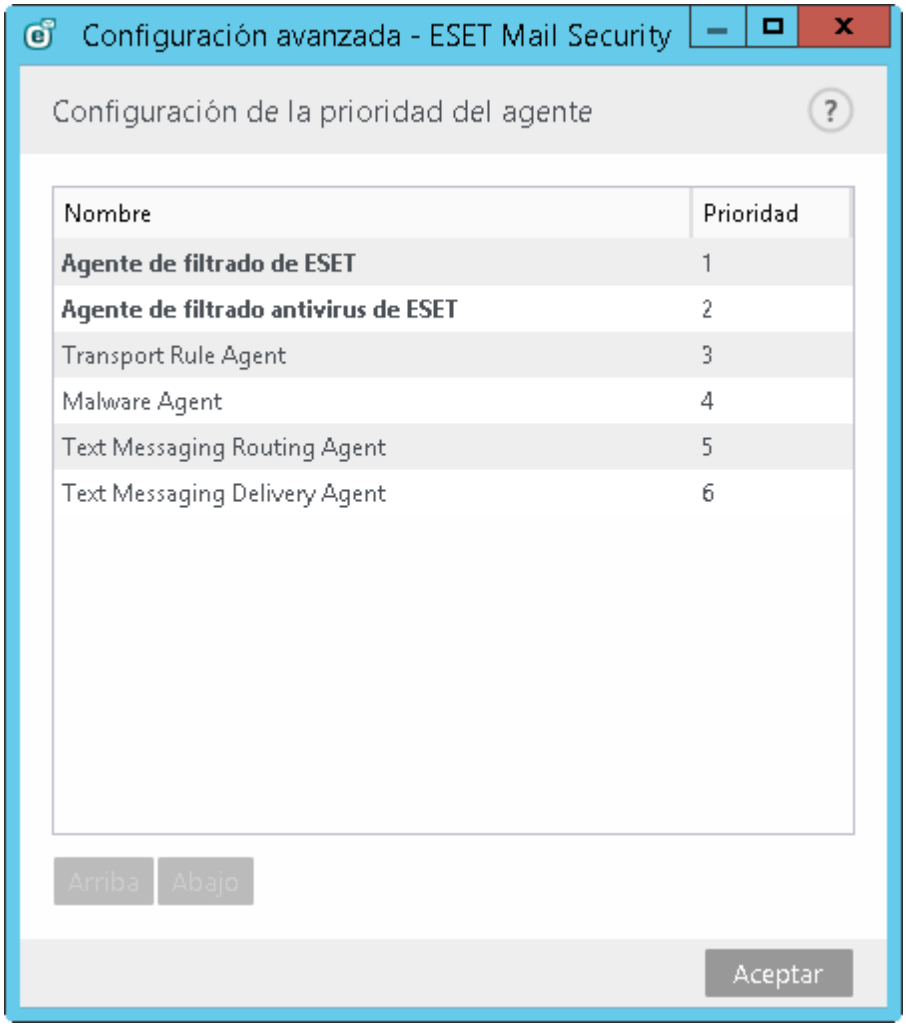
Con Microsoft Exchange Server 2003 puede especificar la prioridad de los agentes de forma independiente utilizando fichas para EOD (fin de los datos) y RCPT (destinatario).

5.1.1.1 Modificar prioridad

Si está ejecutando Microsoft Exchange Server 2003, puede definir el número manualmente para cambiar la **Prioridad del agente de transporte**. Modifique el número en el campo de texto o utilice las flechas arriba y abajo para cambiar la prioridad. Cuanto más bajo es el número, más alta es la prioridad.

5.1.2 Configuración de la prioridad del agente

En el menú **Configuración de prioridad de agentes** puede definir la prioridad con la que los agentes de ESET Mail Security pasan a ser activos después del inicio del servidor de Microsoft Exchange. Esta opción se aplica a Microsoft Exchange 2007 y versiones más recientes.



- **Subir**: suba la posición de un agente seleccionado en la lista de agentes para aumentar su prioridad.

- **Bajar**: baje la posición de un agente seleccionado en la lista de agentes para reducir su prioridad.

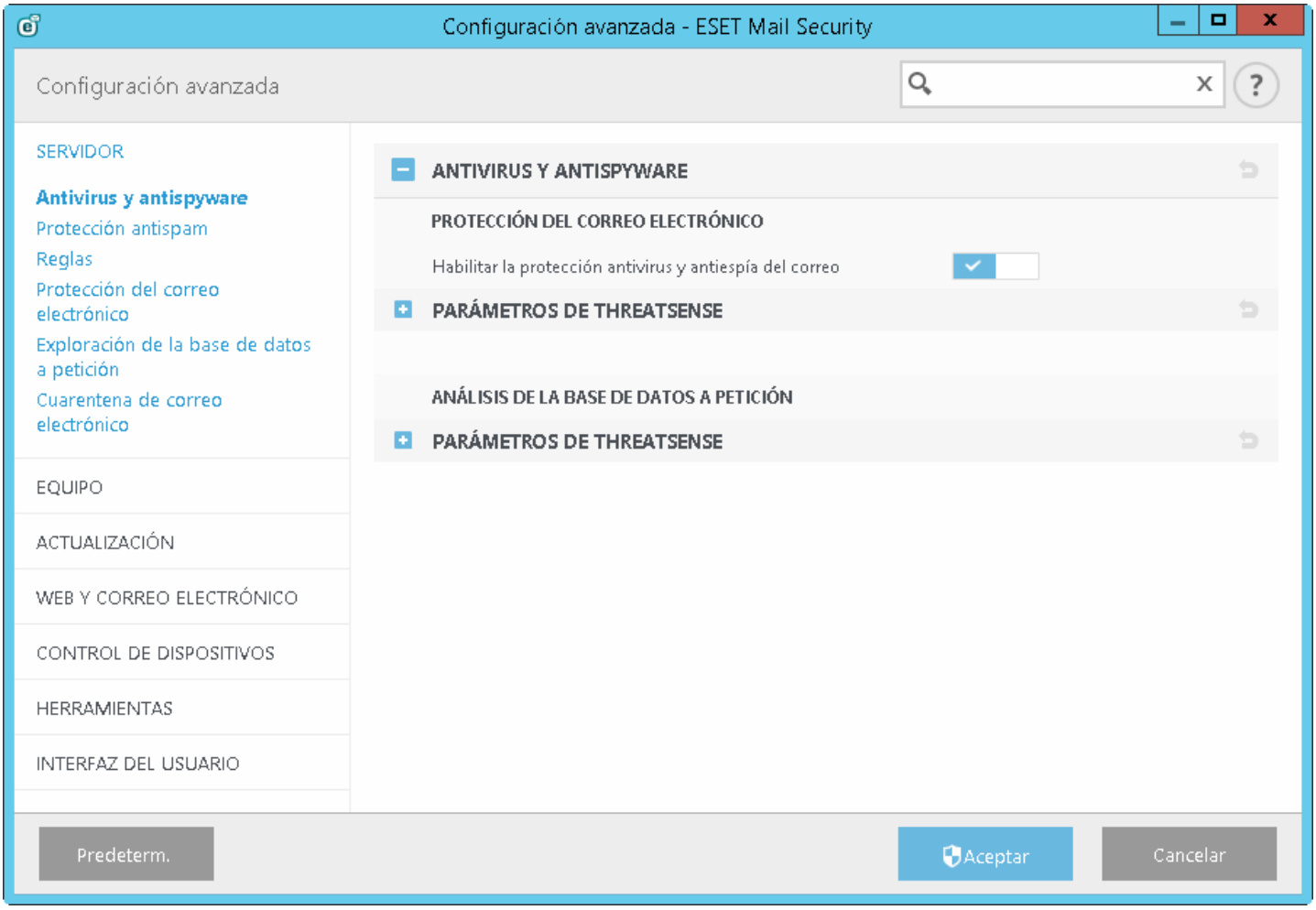
5.1.3 Antivirus y antiespía

En esta sección puede configurar las opciones de **Antivirus y antiespía** de su servidor de correo.

IMPORTANTE: la protección del transporte del correo electrónico la proporciona el agente de transporte; solo está disponible en Microsoft Exchange Server 2007 y versiones posteriores, pero su servidor Exchange Server debe tener el rol Servidor de transporte perimetral o Servidor concentrador de transporte. Esto también se aplica a una instalación con un solo servidor con varios roles de Exchange Server en un ordenador (siempre que incluya el rol de servidor perimetral o concentrador de transporte).

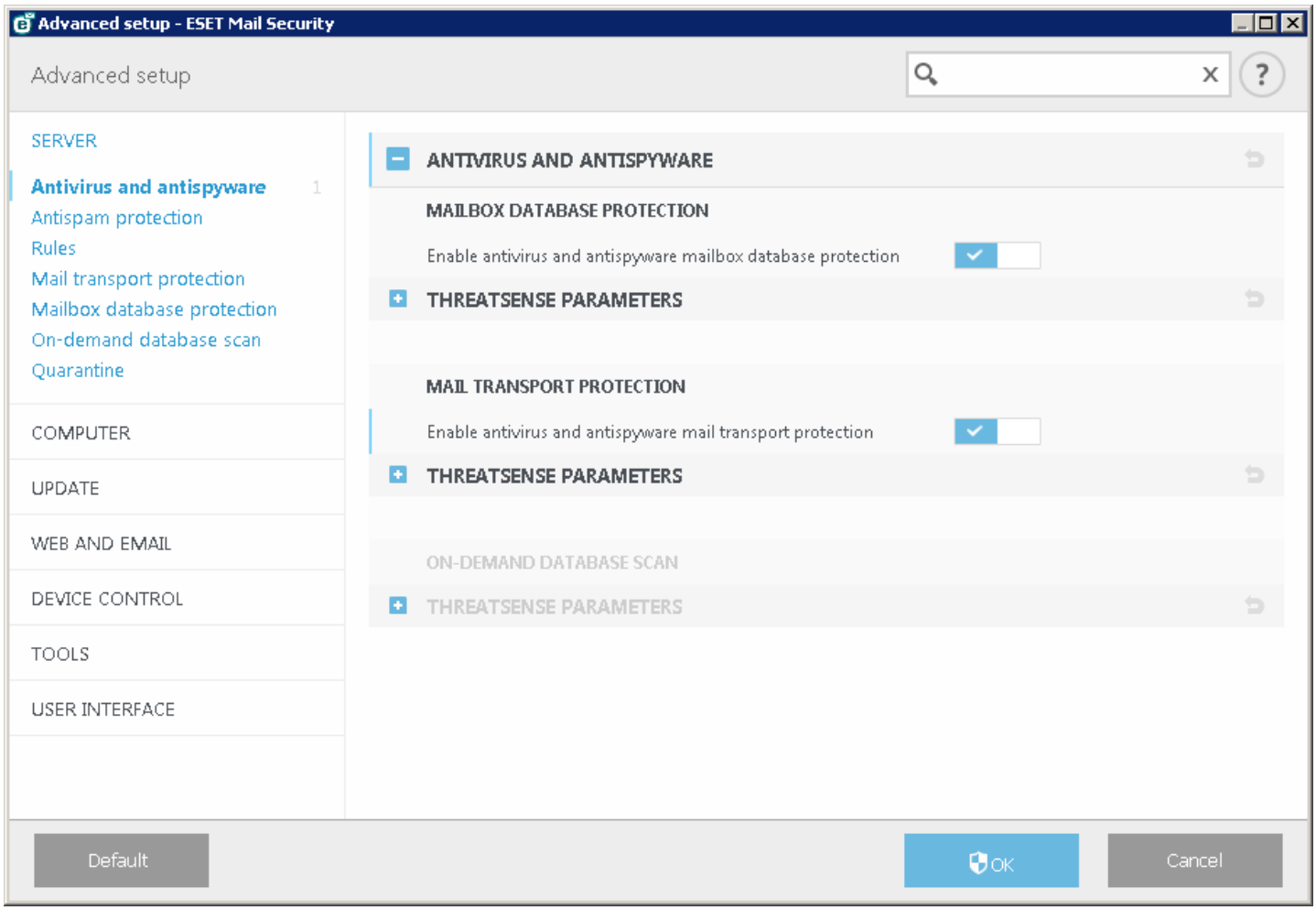
Protección del correo electrónico:

Si desactiva la opción **Habilitar protección antivirus y antispyware del transporte de correo**, el complemento de ESET Mail Security para Exchange Server no se descargará del proceso de Microsoft Exchange Server, simplemente pasará los mensajes sin buscar virus en la capa de transporte. Los mensajes se seguirán analizando en busca de virus y spam en la capa de la base de datos, y se aplicarán las reglas existentes.



Protección de la base de datos de buzones:

Si desactiva la opción **Activar protección antivirus y antiespía de la base de datos de buzones**, el complemento de ESET Mail Security para Exchange Server no se descargará del proceso de Microsoft Exchange Server, simplemente pasará los mensajes sin buscar virus en la capa de la base de datos. Los mensajes se seguirán analizando en busca de virus y spam en la capa de transporte, y se aplicarán las reglas existentes.



5.1.4 Protección Antispam

La protección antispam del servidor de correo está activada de forma predeterminada. Para desactivarla, haga clic en el conmutador situado junto a **Habilitar la protección antispam**.

Activar **Usar listas blancas de Exchange Server para omitir automáticamente la protección antispam** permite que ESET Mail Security utilice "listas blancas" específicas de Exchange. Si está activada, se tendrá en cuenta lo siguiente:

- La dirección IP del servidor está en la lista de IP permitidas de Exchange Server.
- El destinatario del mensaje tiene el indicador No aplicar antispam establecido en su buzón de correo.
- El destinatario del mensaje tiene la dirección del remitente en la lista Remitentes seguros (asegúrese de que ha configurado la sincronización de la lista de remitentes seguros en su entorno de Exchange Server, incluido Agregación de lista segura).

Si alguno de los puntos anteriores se aplica a un mensaje entrante, no se llevará a cabo la comprobación de antispam en dicho mensaje y, por lo tanto, no se evaluará su nivel de SPAM y se entregará en el buzón de entrada del destinatario.

La opción **Aceptar el indicador antispam establecido en sesión de SMTP** es útil cuando hay sesiones SMTP autenticadas entre servidores Exchange con la configuración de No aplicar antispam. Por ejemplo, si tiene un servidor Perimetral y un servidor Concentrador, no es necesario analizar el tráfico entre estos dos servidores. La opción **Aceptar la marca de omisión de antispam establecida por la sesión SMTP** está activada de forma predeterminada y se aplica cuando hay un indicador No aplicar antispam configurado para la sesión SMTP en Exchange Server. Si desactiva la opción **Aceptar la marca de omisión de antispam establecida por la sesión SMTP**, ESET Mail Security analizará la sesión SMTP en busca de spam sea cual sea la configuración de omisión de antispam establecida en Exchange Server.

NOTA: es necesario actualizar la base de datos de antispam periódicamente para que el módulo antispam proporcione la mejor protección posible. Para permitir actualizaciones regulares de la base de datos de antispam, asegúrese de que ESET Mail Security dispone de acceso a las direcciones IP correctas en los puertos necesarios. Para

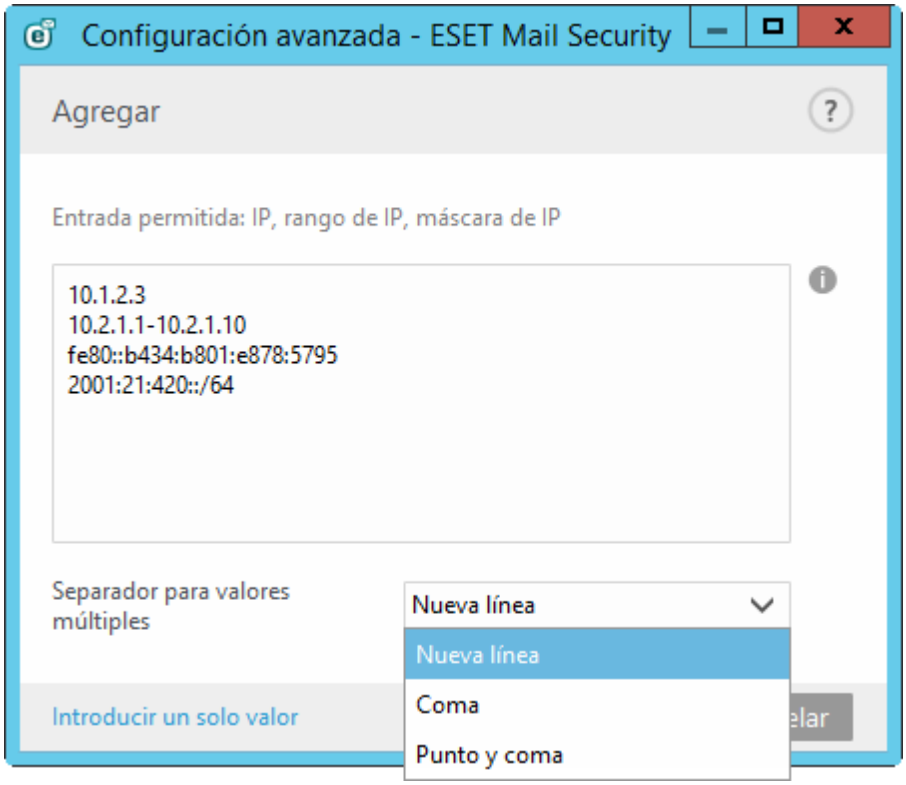
obtener más información sobre las direcciones IP y los puertos que debe activa en el cortafuegos de terceros, lea este artículo de la base de conocimiento.

5.1.4.1 Filtrado y verificación

Puede configurar las listas de **Permitido**, **Bloqueado** e **Ignorado** al especificar criterios como direcciones IP o rango de las mismas, nombres de dominio, etc. Si desea añadir, modificar o eliminar criterios, haga clic en **Editar** junto a la lista que quiera gestionar.

- **Lista de IP autorizadas**: añade automáticamente a la lista blanca los correos electrónicos que tienen su origen en las direcciones IP especificadas.
- **Lista de IP bloqueadas**: bloquea automáticamente los correos electrónicos que tienen su origen en las direcciones IP especificadas.
- **Lista de IP ignoradas**: lista de direcciones IP que se ignorarán durante la clasificación.
- **Lista de dominios con cuerpo bloqueado**: bloquea los mensajes de correo electrónico que contienen el dominio especificado en el cuerpo del mensaje.
- **Lista de dominios con cuerpo ignorado**: los dominios especificados en el cuerpo del mensaje se ignorarán durante la clasificación.
- **Lista de IP con cuerpo bloqueado**: bloquea los mensajes de correo electrónico que contienen la dirección IP especificada en el cuerpo del mensaje.
- **Lista de IP con cuerpo ignorado**: las direcciones IP especificadas en el cuerpo del mensaje se ignorarán durante la clasificación.
- **Lista de remitentes autorizados**: añade a la lista blanca los correos electrónicos procedentes del remitente especificado.
- **Lista de remitentes bloqueados**: bloquea los correos electrónicos procedentes del remitente especificado.
- **Dominio aprobado en lista de IP**: añade a la lista blanca los correos electrónicos que tienen su origen en direcciones IP que se resuelven desde los dominios especificados en esta lista.
- **Dominio bloqueado en lista de IP**: bloquea los correos electrónicos que tienen su origen en direcciones IP que se resuelven desde los dominios especificados en esta lista.
- **Dominio ignorado en lista de IP**: lista de dominios que resuelven en direcciones IP que, a su vez, no se comprobarán durante la clasificación.
- **Lista de conjuntos de caracteres bloqueados**: bloquea los correos electrónicos que tienen los conjuntos de caracteres especificados.
- **Lista de países bloqueados**: bloquea los correos electrónicos procedentes de los países especificados.

NOTA: Si desea agregar más entradas a la vez, haga clic en **Introduzca múltiples valores** en la ventana emergente Agregar y elija qué separador se debe usar; puede ser **Nueva línea**, **Coma** o **Punto y coma**. Por ejemplo:



5.1.4.2 Configuración avanzada

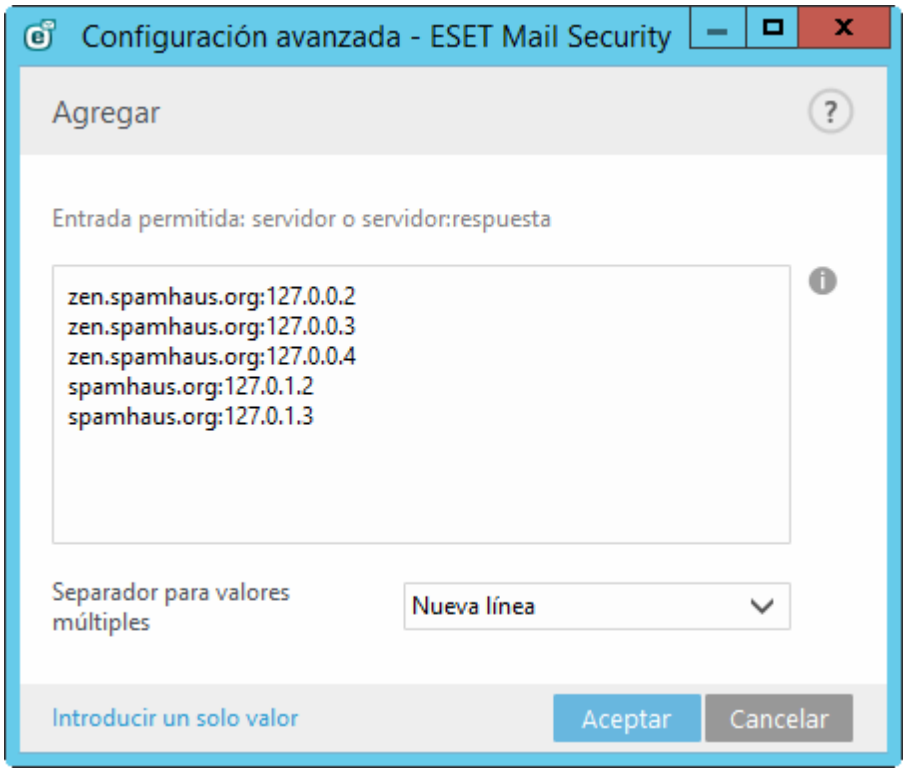
Esta configuración permite que servidores externos (**RBL**, lista de bloqueo en tiempo real, **DNSBL**, lista de bloqueados de DNS) verifiquen los mensajes según los criterios definidos.

Número máximo de direcciones verificadas desde los encabezados Recibidos: : puede limitar el número de direcciones IP que comprueba la protección antispam. Esto hace referencia a las direcciones IP escritas en los encabezados de `Received: from`. El valor predeterminado es 0, lo que supone sin límite.

Compruebe si la dirección del remitente aparece en la lista negra de usuarios finales.: los mensajes de correo electrónico que no se envían desde servidores de correo (desde ordenadores que no están marcados como servidores de correo) se verifican para asegurar que el remitente no se encuentra en la lista negra. Esta opción está activada de forma predeterminada. Si lo desea puede desactivarla, pero los mensajes que no se envíen desde servidores de correo no se comprobarán con la lista negra.

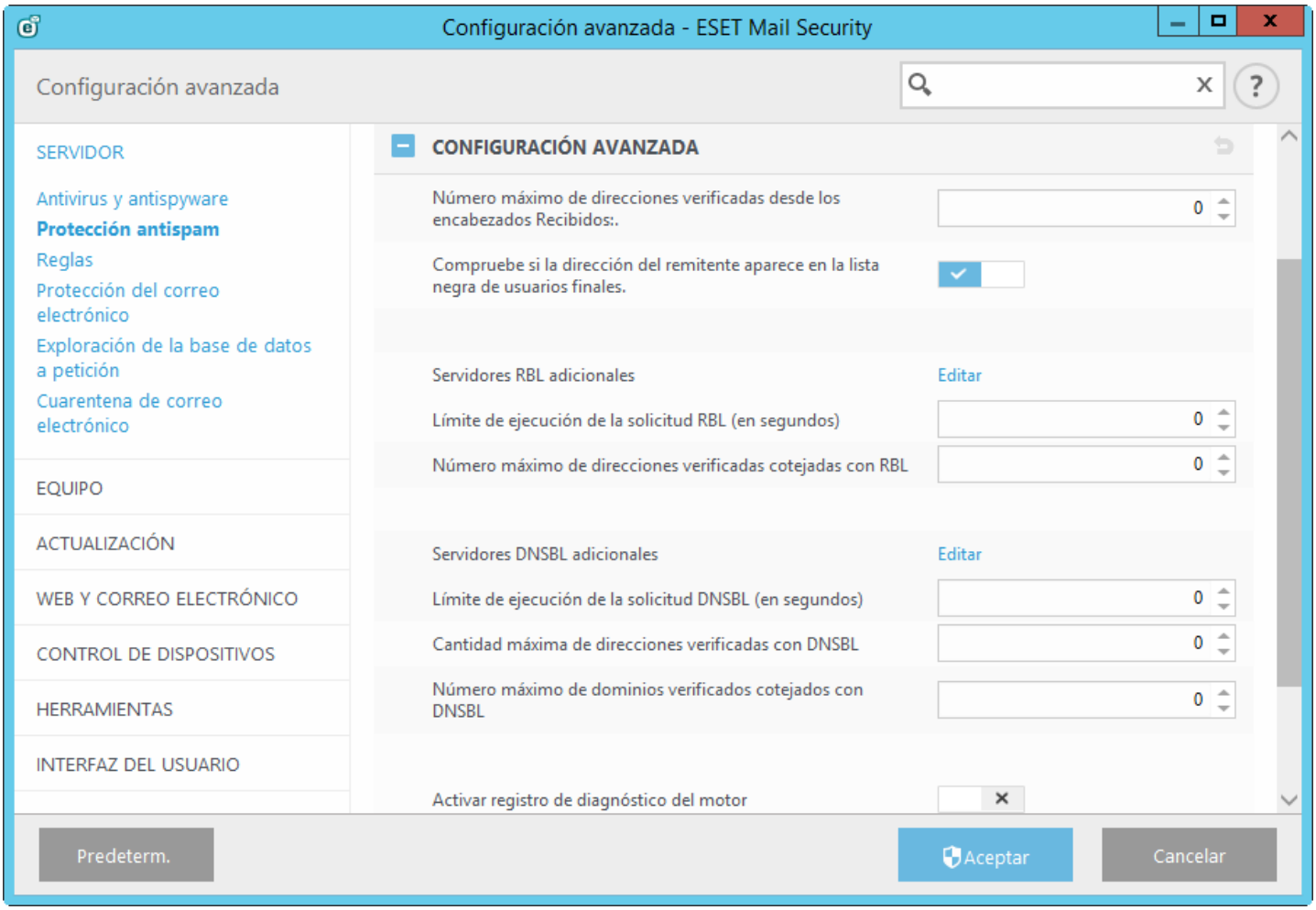
Servidores RBL adicionales: se trata de una lista de los servidores de bloqueo en tiempo real (RBL) que se consulta al analizar los mensajes.

NOTA: cuando añada servidores RBL adicionales, especifique el nombre de dominio del servidor con un código de devolución con el formato `servidor:respuesta` (p. ej. `zen.spamhaus.org:127.0.0.4`). Además, añada cada nombre de servidor y código de devolución por separado, para lograr una lista completa. Haga clic en **Introduzca múltiples valores** en la ventana emergente Agregar para especificar todos los nombres de servidor con sus códigos de devolución. Las entradas deben tener el mismo aspecto que el de este ejemplo; los códigos de devolución y los nombres de host del servidor RBL reales pueden variar:



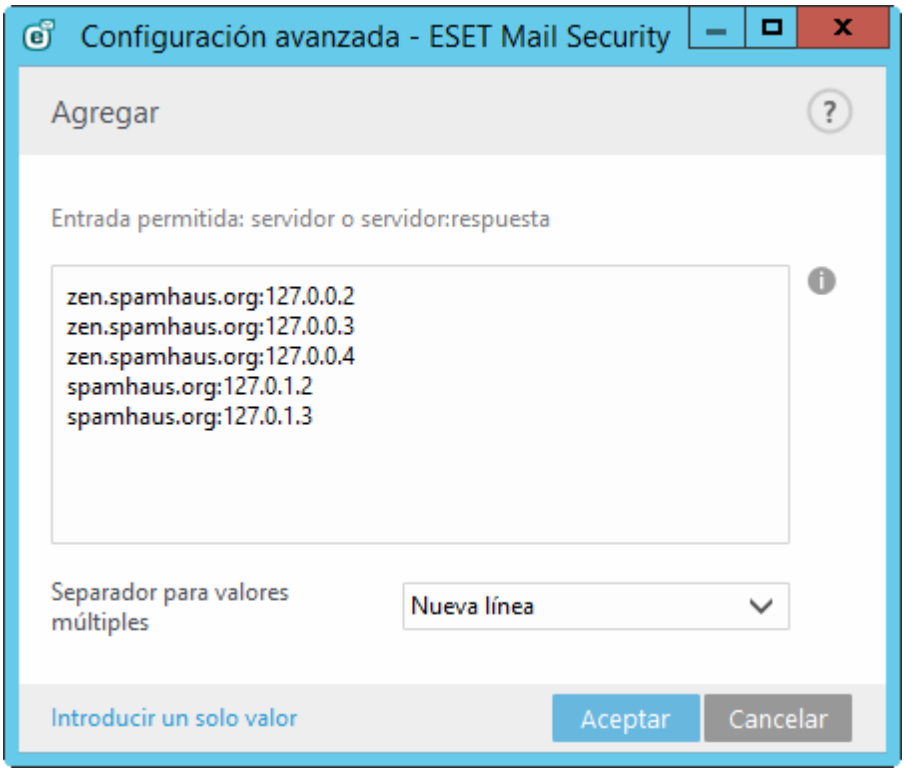
Límite de ejecución de la solicitud RBL (en segundos): esta opción le permite establecer un tiempo máximo para las consultas de RBL. Solo se utilizan las respuestas RBL de los servidores RBL que responden a tiempo. Si el valor está establecido en "0", no se aplica tiempo de espera.

Número máximo de direcciones verificadas cotejadas con RBL: esta opción le permite limitar el número de direcciones IP que se consultan en el servidor RBL. Tenga en cuenta que el número total de consultas RBL será el número de direcciones IP de los encabezados Recibido: (hasta un máximo de direcciones IP de verificación de RBL) multiplicado por el número de servidores RBL especificado en la lista RBL. Si el valor está establecido en "0", se verifica la cantidad ilimitada de encabezados recibidos. Recuerde que las direcciones IP de la lista de direcciones IP ignoradas no se computarán para el límite de direcciones IP de RBL.



Servidores DNSBL adicionales: es una lista de servidores de lista de bloqueados de DNS (DNSBL) para la consulta sobre dominios y direcciones IP extraídos del cuerpo del mensaje.

NOTA: cuando añada servidores DNSBL adicionales, especifique el nombre de dominio del servidor con un código de devolución con el formato `servidor:respuesta` (p. ej. `zen.spamhaus.org:127.0.0.4`). Además, añada cada nombre de servidor y código de devolución por separado, para lograr una lista completa. Haga clic en **Introduzca múltiples valores** en la ventana emergente Agregar para especificar todos los nombres de servidor con sus códigos de devolución. Las entradas deben tener el mismo aspecto que el de este ejemplo; los códigos de devolución y los nombres de host del servidor DNSBL reales pueden variar:



Límite de ejecución de la solicitud DNSBL (en segundos): le permite establecer un tiempo de espera máximo para que finalicen todas las consultas de DNSBL.

Cantidad máxima de direcciones verificadas con DNSBL: esta opción le permite limitar el número de direcciones IP que se consultan en el servidor de lista de bloqueo de DNS.

Número máximo de dominios verificados cotejados con DNSBL: esta opción le permite limitar el número de dominios que se consultan en el servidor de lista de bloqueo de DNS.

Activar registro de diagnóstico del motor: escribe información detallada sobre el motor antispam en los archivos de registro con fines de diagnóstico.

Tamaño máximo del mensaje analizado (kB): ignora en el análisis antispam los mensajes que tienen un tamaño superior al valor especificado. El motor antispam no analizará estos mensajes. Comportamiento:

Si el Tamaño máximo del mensaje analizado está configurado en: 0 = análisis ilimitado
Si el Tamaño máximo del mensaje analizado está configurado en: 1 - 12288 = 12288
Si el Tamaño máximo del mensaje analizado está configurado en: más de 12288 = valor establecido
El valor mínimo recomendado es 100 kB.

5.1.4.3 Configuración de lista gris

La función **Activar creación de listas grises** activa una característica que protege a los usuarios frente al correo no deseado con la técnica siguiente: El agente de transporte enviará un valor de retorno SMTP "rechazar temporalmente" (el valor predeterminado es 451/4.7.1) para los mensajes recibidos que no procedan de un remitente conocido. Los servidores legítimos intentarán enviar el mensaje otra vez tras una demora. Por lo general, los servidores de spam no intentan enviar el mensaje otra vez, ya que suelen pasar por miles de direcciones de correo electrónico y no pierden el tiempo con reenvíos. Las listas grises son una capa adicional de la protección antispam y no tienen ningún efecto sobre la capacidad de evaluación del correo no deseado del módulo antispam.

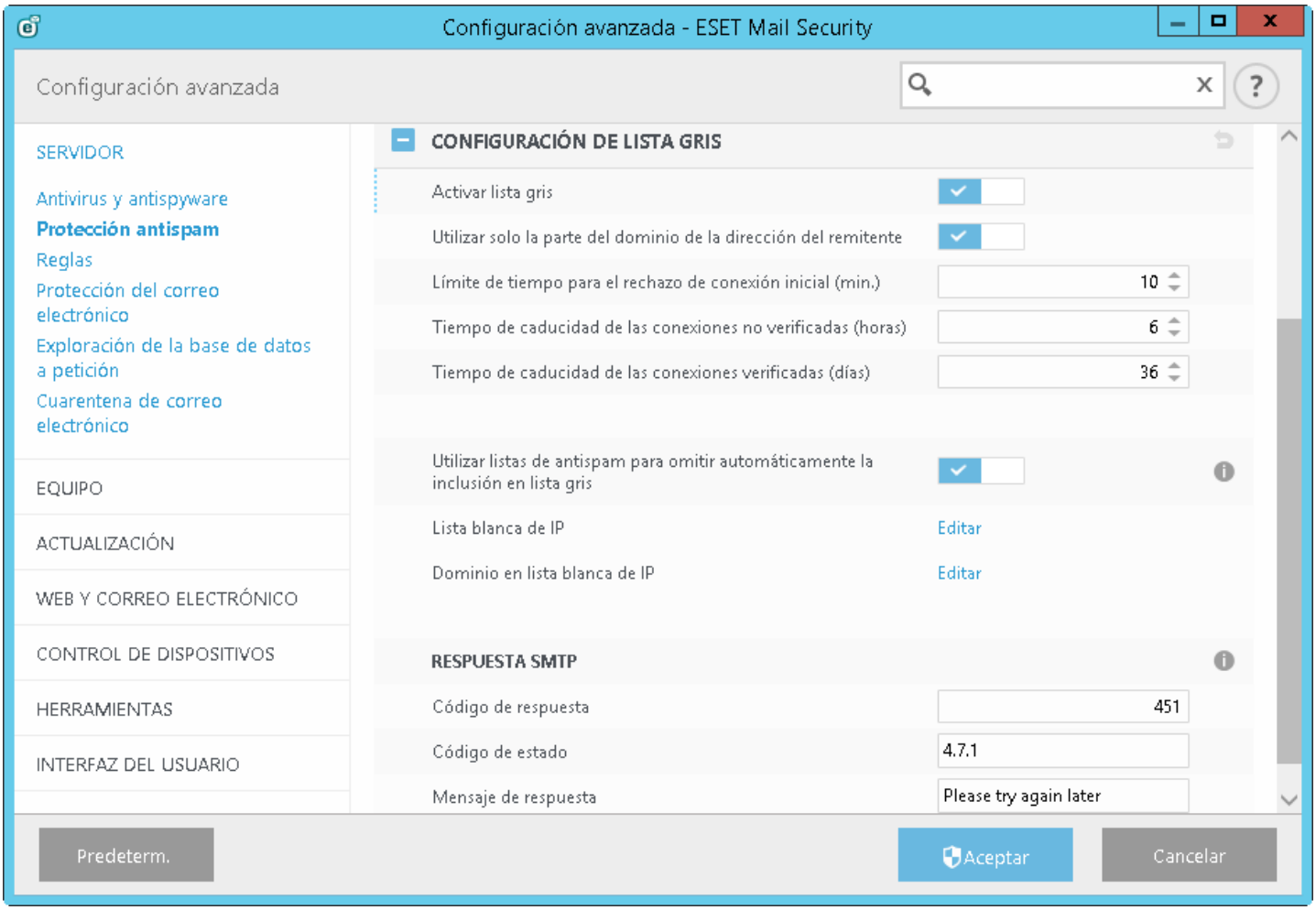
Cuando evalúa el origen del mensaje, el método de lista gris tiene en cuenta las listas de **IP permitidas**, **IP ignoradas**, **Remitentes seguros** y **Permitir IP** de Exchange Server y la configuración de No aplicar antispam del buzón de correo del destinatario. El método de detección de listas grises omitirá los correos electrónicos procedentes de estas listas de remitentes y direcciones IP o entregados a un buzón de correo que tiene activada la opción No aplicar antispam.

Utilizar solo la parte del dominio de la dirección del remitente: ignora el nombre del destinatario en la dirección de correo electrónico, solo se tiene en cuenta el dominio.

Límite de tiempo para el rechazo de conexión inicial (min.): cuando un mensaje se entrega por primera vez y se rechaza de forma temporal, este parámetro define el período de tiempo durante el que siempre se rechazará el mensaje (a partir del primer rechazo). Una vez que este periodo haya transcurrido, el mensaje se recibirá correctamente. El valor mínimo es 1 minuto.

Tiempo de caducidad de las conexiones no verificadas (horas): este parámetro define el intervalo de tiempo mínimo durante el que se guardarán los datos de los tres elementos. Un servidor válido debe reenviar el mensaje enviado antes de que finalice este periodo. Este valor debe ser mayor que el valor de **Límite de tiempo para el rechazo de conexión inicial**.

Tiempo de caducidad de las conexiones verificadas (días): el número mínimo de días que se guardan los datos de los tres elementos, y durante los cuales los mensajes de correo electrónico de un remitente determinado se reciben sin demora. Este valor debe ser mayor que el valor de **Tiempo de caducidad de las conexiones no verificadas**.


Configuración avanzada - ESET Mail Security
Configuración avanzada
SERVIDOR
Antivirus y antispyware
Protección antispam
Reglas
Protección del correo electrónico
Exploración de la base de datos a petición
Cuarentena de correo electrónico
EQUIPO
ACTUALIZACIÓN
WEB Y CORREO ELECTRÓNICO
CONTROL DE DISPOSITIVOS
HERRAMIENTAS
INTERFAZ DEL USUARIO
CONFIGURACIÓN DE LISTA GRIS
Activar lista gris
Utilizar solo la parte del dominio de la dirección del remitente
Límite de tiempo para el rechazo de conexión inicial (min.) 10
Tiempo de caducidad de las conexiones no verificadas (horas) 6
Tiempo de caducidad de las conexiones verificadas (días) 36
Utilizar listas de antispam para omitir automáticamente la inclusión en lista gris
Lista blanca de IP Editar
Dominio en lista blanca de IP Editar
RESPUESTA SMTP
Código de respuesta 451
Código de estado 4.7.1
Mensaje de respuesta Please try again later
Predeterm.
Aceptar
Cancelar

Respuesta SMTP (para conexiones denegadas temporalmente): puede especificar valores de **Código de respuesta**, **Código de estado** y **Mensaje de respuesta** que definen la respuesta de denegación de SMTP temporal enviada al servidor SMTP si se rechaza un mensaje.

Ejemplo de mensaje de respuesta de rechazo de SMTP:

Código de respuesta	Código de estado	Mensaje de respuesta
451	4.7.1	Se canceló la acción solicitada: error local al procesar

ADVERTENCIA: una sintaxis incorrecta en los códigos de respuesta SMTP podría provocar el mal funcionamiento de la protección proporcionada por las listas grises. Por ello, es posible que los mensajes no deseados se entreguen a los clientes o que los mensajes no se entreguen nunca.

NOTA: en la definición de respuestas SMTP de rechazo también puede utilizar variables del sistema.

5.1.5 Reglas

Las **Reglas** permiten a los administradores definir manualmente las condiciones de filtrado de correo electrónico y las acciones que se deben realizar con los mensajes de correo electrónico filtrados.

Existen tres conjuntos de reglas independientes. Las reglas disponibles en el sistema dependen de la versión de Microsoft Exchange Server instalada en el servidor con ESET Mail Security:

- Protección de la base de datos de buzones: este tipo de protección solo está disponible para Microsoft Exchange Server 2010, 2007 y 2003 en funcionamiento en los roles Servidor de buzones (Microsoft Exchange 2010 y 2007) o Servidor administrativo (Microsoft Exchange 2003). Este tipo de análisis puede realizarse en una instalación con un solo servidor con varios roles de Exchange Server en un ordenador (siempre que incluya el rol de buzones de correo o administrativo).
- Protección del correo electrónico: esta protección la proporciona el agente de transporte, y solo está disponible para Microsoft Exchange Server 2007 o versiones más recientes con el rol Servidor de transporte perimetral o Servidor concentrador de transporte. Este tipo de análisis puede realizarse en una instalación con un solo servidor con varios roles de Exchange Server en un ordenador (siempre que incluya uno de los roles de servidor mencionados).
- Análisis de la base de datos a petición: le permite ejecutar o programar un análisis de la base de datos de buzones de correo. Esta función solo está disponible en Microsoft Exchange Server 2007 o versiones más recientes con el rol Servidor de buzones de correo o Concentrador de transporte. Esto también se aplica a una instalación con un solo servidor con varios roles de Exchange Server en un ordenador (siempre que incluya uno de los roles de servidor mencionados). Consulte Roles de Exchange Server 2013 para acceder a información específica sobre los roles de Exchange 2013.

5.1.5.1 Lista de reglas

Una regla está compuesta por **condiciones** y **acciones**. Cuando se cumplan todas las condiciones de un mensaje de correo electrónico se realizarán acciones con ese mensaje de correo electrónico. En otras palabras, las reglas se aplican en función de un grupo de condiciones combinadas. Si existen varias condiciones para una regla, estas se combinarán utilizando el operador lógico AND y la regla solo se aplicará si se cumplen las condiciones.

En la ventana de lista **Reglas** se muestran las reglas existentes. Las reglas se clasifican en tres niveles, y se evalúan en este orden:

- **Reglas de filtrado (1)**
- **Reglas de procesamiento de adjuntos (2)**
- **Reglas de procesamiento de resultados (3)**

Las reglas del mismo nivel se evalúan en el mismo orden que se muestran en la ventana de reglas. Solo puede cambiar el orden de reglas de aquellas reglas que se encuentran en el mismo nivel. Por ejemplo, cuando dispone de varias reglas de filtrado, puede cambiar el orden en el que se aplican. No puede cambiar su orden al establecer las reglas de Procesamiento de adjuntos antes de las reglas de Filtrado, los botones Arriba/Abajo no estarán disponibles. En otras palabras, no puede combinar reglas de niveles distintos.

La columna Coincidencias muestra el número de veces que la regla se ha aplicado correctamente. Desmarcar una casilla de verificación (a la izquierda del nombre de cada regla) desactiva la regla correspondiente hasta que la marca de nuevo.

- **Agregar...** : agrega una regla nueva.
- **Editar...** : modifica una regla existente.
- **Quitar**: elimina la regla seleccionada.
- **Subir**: sube la posición de la regla seleccionada en la lista.
- **Bajar**: baja la posición de la regla seleccionada en la lista.
- **Restablecer**: restablece el contador de la regla seleccionada (la columna Coincidencias).

NOTA: si se ha agregado una regla nueva o se ha modificado una regla existente, se iniciará automáticamente un nuevo análisis de mensajes con las reglas nuevas o modificadas.

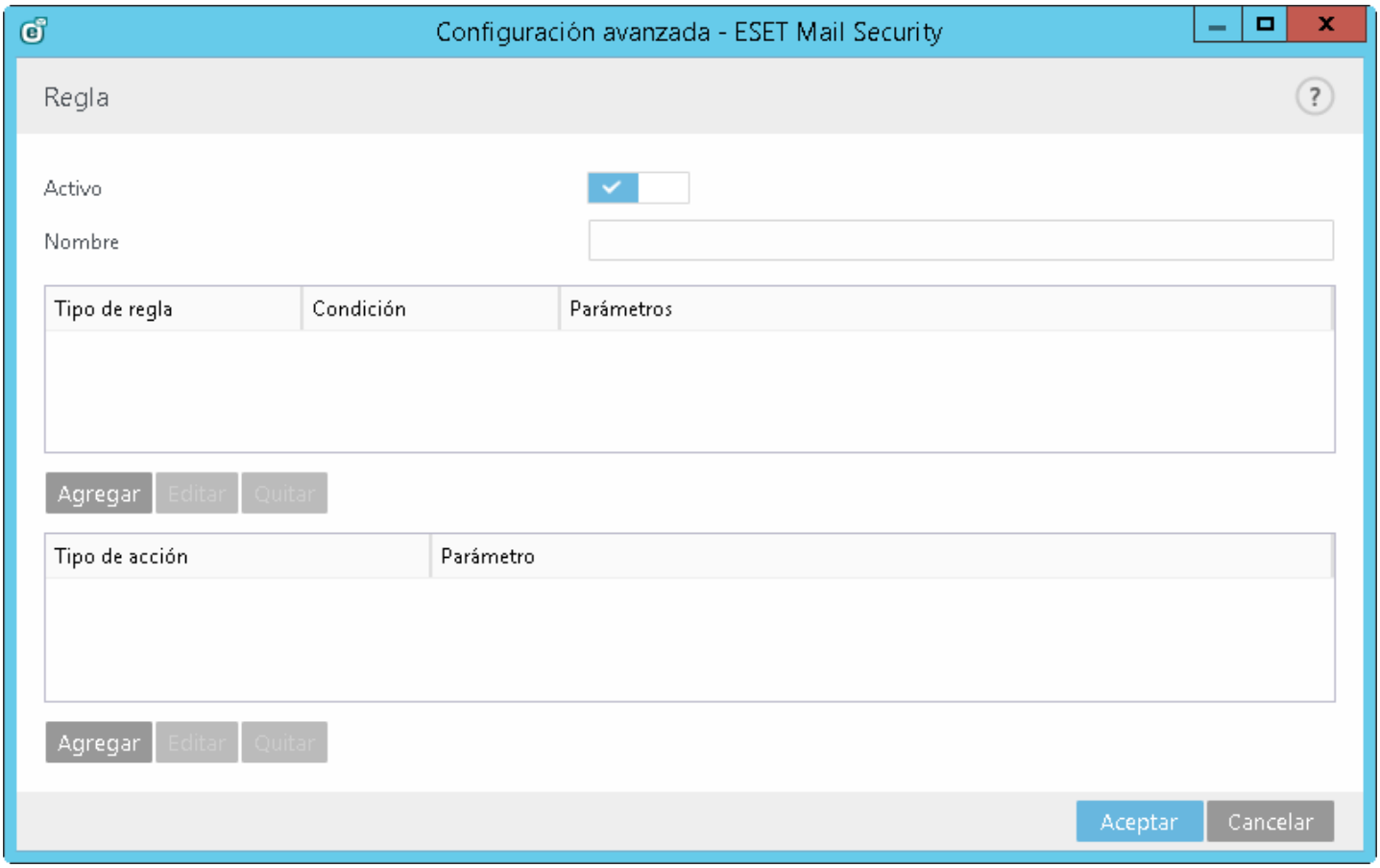
Las reglas se cotejan con un mensaje cuando el agente de transporte (AT) o VSAPI lo procesan. Si están activados el agente de transporte y VSAPI, y el mensaje cumple las condiciones de la regla, el contador de la regla puede aumentar en 2 o más. Esto se debe a que VSAPI accede al cuerpo y al adjunto del mensaje por separado, y por ello las reglas se aplican a cada elemento por separado. Las reglas también se aplican durante el análisis en segundo plano (por ejemplo, cuando ESET Mail Security realiza un análisis de buzones tras la descarga de una nueva base de firmas de virus), lo que puede aumentar el contador de reglas.

5.1.5.1.1 Asistente de reglas

Puede definir **Condiciones** y **Acciones** utilizando el **Asistente de reglas**. Defina primero las condiciones y, a continuación, las acciones. Haga clic en **Agregar** y aparecerá una ventana de Condición de regla en la que puede seleccionar el tipo de condición, la operación y el valor. Desde aquí puede agregar una Acción de regla. Una vez definidas las condiciones y las acciones, escriba un **Nombre** para la regla (elija una opción por la que reconocerá la regla); este nombre se mostrará en la Lista de reglas. Si quiere preparar las reglas pero tiene previsto utilizarlas posteriormente, puede hacer clic en el conmutador situado junto a **Activa** para desactivar la regla. Si desea activar la regla, marque la casilla de verificación situada junto a la regla que desee activar desde la Lista de reglas.

NOTA: **Nombre** es un campo obligatorio; si está resaltado en rojo, escriba el nombre de la regla en el cuadro de texto y haga clic en el botón **Aceptar** para crear la regla. El resaltado en rojo no desaparece ni siquiera después de introducir el nombre de la regla, solo desaparece cuando hace clic en **Aceptar**.

Algunas **Condiciones** y **Acciones** son distintas en las reglas específicas de la **Protección del correo electrónico**, la **Protección de la base de datos de buzones** y el **Análisis de la base de datos a petición**. Esto se debe a que cada uno de estos tipos de protección usa un enfoque ligeramente distinto al procesar los mensajes, especialmente la **Protección del correo electrónico**.



NOTA: Si configura el tipo de acción **Registro de sucesos** para la protección de la base de datos de buzones con el parámetro %IPAddress%, la columna **Suceso** de los archivos de registro estará vacía para este suceso en concreto. Esto se debe a que no hay dirección IP en el nivel de protección de la base de datos de buzones. Algunas opciones no están disponibles en todos los niveles de protección:

Dirección IP: se ignora en **Análisis de la base de datos a petición** y **Protección de la base de datos de buzones**
Buzón: se ignora en **Protección del transporte del correo electrónico**

5.1.5.1.1.1 Condición de la regla

Este asistente le permite agregar las condiciones de una regla. Seleccione **Tipo** > **Operación** en la lista desplegable (la lista de operaciones cambia en función del tipo de regla seleccionado) y elija **Parámetro**. Los campos de parámetros cambiarán en función del tipo de regla y la operación.

Por ejemplo, elija **Tamaño del archivo adjunto** > **es mayor que** y, bajo **Parámetro**, especifique 10 MB. Con esta configuración, todo aquel mensaje que contenga un archivo adjunto con un tamaño superior a los 10 MB se procesará con la acción de regla que haya especificado. Por este motivo, debe especificar la acción que se realiza cuando se desencadena una regla determinada, si no lo ha hecho al configurar los parámetros de dicha regla.

NOTA: es posible agregar varias condiciones para una regla. Cuando se agreguen varias condiciones, aquellas condiciones que anulen otras no se mostrarán.

Las siguientes **Condiciones** están disponibles para la **Protección del correo electrónico** (algunas opciones podrían no mostrarse, en función de las condiciones anteriormente seleccionadas):

- **Asunto**: se aplica a los mensajes que contienen o no contienen una cadena concreta (o una expresión regular) en el asunto.
- **Remitente**: se aplica a los mensajes enviados por un remitente concreto.
- **Destinatario**: se aplica a los mensajes enviados a un destinatario concreto.
- **Nombre del archivo adjunto**: se aplica a los mensajes que contienen archivos adjuntos con un nombre concreto.
- **Tamaño del archivo adjunto**: se aplica a los mensajes que contienen un archivo adjunto que no cumple con un tamaño especificado, está dentro de un intervalo de tamaño especificado o supera un tamaño especificado.
- **Tipo de archivo adjunto**: se aplica a aquellos mensajes que tienen un tipo de archivo concreto adjunto. Los tipos de archivo se clasifican en grupos para facilitar su selección, puede seleccionar varios tipos de archivo o categorías completas.
- **Tamaño del mensaje**: se aplica a los mensajes que contienen archivos adjuntos que no cumplen con un tamaño especificado, están dentro de un intervalo de tamaño especificado o superan un tamaño especificado.
- **Resultado del análisis antispam**: se aplica a aquellos mensajes marcados o no marcados como spam.
- **Resultado del análisis antivirus**: se aplica a los mensajes marcados como maliciosos o no maliciosos.
- **Mensaje interno**: se aplica en función de si el mensaje es interno o no interno.
- **Hora de recepción**: se aplica a los mensajes recibidos antes o después de una fecha específica, o durante un intervalo de fechas específico.
- **Encabezados del mensaje**: se aplica a mensajes con datos específicos presentes en el encabezado del mensaje.
- **Contiene un archivo comprimido protegido por contraseña**: se aplica a los mensajes que contienen archivos adjuntos comprimidos protegidos por medio de una contraseña.
- **Contiene un archivo comprimido dañado**: se aplica a los mensajes que contienen archivos adjuntos comprimidos dañados (y que probablemente no pueden abrirse).
- **Dirección IP del remitente**: se aplica a los mensajes enviados desde una dirección IP concreta.
- **Dominio del remitente**: se aplica a los mensajes procedentes de un remitente con un dominio específico en sus direcciones de correo electrónico.

- **Unidades organizativas del destinatario**: se aplica a los mensajes enviados a un destinatario de una unidad organizativa específica.

Lista de condiciones disponibles para Protección de la base de datos de buzones y Análisis de la base de datos a petición (algunas de las opciones podrían no mostrarse en función de las condiciones anteriormente seleccionadas):

- **Asunto**: se aplica a los mensajes que contienen o no contienen una cadena concreta (o una expresión regular) en el asunto.
- **Remitente**: se aplica a los mensajes enviados por un remitente concreto.
- **Destinatario**: se aplica a los mensajes enviados a un destinatario concreto.
- **Buzón**: se aplica a los mensajes situados en un buzón concreto.
- **Nombre del archivo adjunto**: se aplica a los mensajes que contienen archivos adjuntos con un nombre concreto.
- **Tamaño del archivo adjunto**: se aplica a los mensajes que contienen un archivo adjunto que no cumple con un tamaño especificado, está dentro de un intervalo de tamaño especificado o supera un tamaño especificado.
- **Tipo de archivo adjunto**: se aplica a aquellos mensajes que tienen un tipo de archivo concreto adjunto. Los tipos de archivo se clasifican en grupos para facilitar su selección, puede seleccionar varios tipos de archivo o categorías completas.
- **Resultado del análisis antivirus**: se aplica a los mensajes marcados como maliciosos o no maliciosos.
- **Hora de recepción**: se aplica a los mensajes recibidos antes o después de una fecha específica, o durante un intervalo de fechas específico.
- **Encabezados del mensaje**: se aplica a mensajes con datos específicos presentes en el encabezado del mensaje.
- **Contiene un archivo comprimido protegido por contraseña**: se aplica a los mensajes que contienen archivos adjuntos comprimidos protegidos por medio de una contraseña.
- **Contiene un archivo comprimido dañado**: se aplica a los mensajes que contienen archivos adjuntos comprimidos dañados (y que probablemente no pueden abrirse).
- **Dirección IP del remitente**: se aplica a los mensajes enviados desde una dirección IP concreta.
- **Dominio del remitente**: se aplica a los mensajes procedentes de un remitente con un dominio específico en sus direcciones de correo electrónico.

5.1.5.1.1.2 Acción de la regla

Puede añadir acciones que se realizarán con los mensajes o los adjuntos que coincidan con las condiciones de la regla.

NOTA: es posible agregar varias condiciones para una regla. Cuando se agreguen varias condiciones, aquellas condiciones que anulen otras no se mostrarán.

La lista de **Acciones** disponibles para la **Protección del correo electrónico** (algunas opciones podrían no mostrarse, en función de las condiciones seleccionadas):

- **Mensaje en cuarentena**: el mensaje no se entregará al destinatario, y se moverá a la cuarentena de correo electrónico.
- **Eliminar archivo adjunto**: elimina el archivo adjunto del mensaje; el mensaje se entregará al destinatario sin el archivo adjunto.
- **Rechazar mensaje**: el mensaje no se entregará y se enviará al remitente un Informe de no entrega (NDR).
- **Ignorar mensaje de forma silenciosa**: elimina el mensaje sin enviar un NDR.

- **Establecer valor de SCL**: cambia o establece un valor de SCL específico.
- **Enviar una notificación por correo electrónico**: envía una notificación por correo electrónico.
- **Omitir análisis antispam**: el motor antispam analizará el mensaje.
- **Omitir análisis antivirus**: el motor antivirus analizará el mensaje.
- **Evaluar otras reglas**: permite la evaluación de otras reglas, de modo que el usuario puede definir varios conjuntos de condiciones y varias acciones en función de las condiciones.
- **Registrar en sucesos**: registra información sobre la regla aplicada en el registro del programa.
- **Añadir campo del encabezado**: añade una cadena personalizada al encabezado de un mensaje.

Lista de **acciones** disponibles para **Protección de la base de datos de buzones** y **Análisis de la base de datos a petición** (algunas de las opciones podrían no mostrarse en función de las condiciones seleccionadas):

- **Eliminar archivo adjunto**: elimina el archivo adjunto del mensaje; el mensaje se entregará al destinatario sin el archivo adjunto.
- **Poner archivo adjunto en cuarentena**: coloca el archivo adjunto al correo electrónico en la cuarentena de correo electrónico, este se entregará al destinatario sin el archivo adjunto.
- **Reemplazar archivo adjunto con información de la acción**: elimina un archivo adjunto y añade información sobre la acción realizada con el archivo adjunto en el cuerpo del correo electrónico.
- **Eliminar mensaje**: elimina el mensaje.
- **Enviar una notificación por correo electrónico**: envía una notificación por correo electrónico.
- **Omitir análisis antivirus**: el motor antivirus analizará el mensaje.
- **Evaluar otras reglas**: permite la evaluación de otras reglas, de modo que el usuario puede definir varios conjuntos de condiciones y varias acciones en función de las condiciones.
- **Registrar en sucesos**: registra información sobre la regla aplicada en el registro del programa.
- **Mover mensaje a la papelera** (solo disponible para el **Análisis de la base de datos a petición**): coloca un mensaje de correo electrónico en la carpeta de papelera del cliente de correo electrónico.

5.1.6 Protección de la base de datos de buzones

Los siguientes sistemas tienen la opción **Protección de la base de datos de buzones** disponible en **Configuración avanzada** > **Servidor**:

- Microsoft Exchange Server 2003 (rol de servidor administrativo)
- Microsoft Exchange Server 2003 (instalación de un solo servidor con varios roles)
- Microsoft Exchange Server 2007 (rol de servidor de buzones)
- Microsoft Exchange Server 2007 (instalación de un solo servidor con varios roles)
- Microsoft Exchange Server 2010 (rol de servidor de buzones)
- Microsoft Exchange Server 2010 (instalación de un solo servidor con varios roles)
- Windows Small Business Server 2003
- Windows Small Business Server 2008
- Windows Small Business Server 2011

NOTA: La protección de la base de datos de buzones no está disponible para Microsoft Exchange Server 2013.

Si desmarca la opción **Activar la protección antivirus y antiespía VSAPI 2.6**, el complemento de ESET Mail Security para Exchange Server no se descargará del proceso de Microsoft Exchange Server, simplemente pasará los mensajes sin buscar virus. No obstante, los mensajes sí se analizarán para detectar el spam y se aplicarán las reglas.

Si está activada la opción **Análisis proactivo**, los nuevos mensajes entrantes se analizarán en el orden de recepción.

Si esta opción está activada y un usuario abre un mensaje que aún no se ha analizado, este mensaje se analizará antes que los demás mensajes de la cola.

El **Análisis en segundo plano** permite que el análisis de todos los mensajes se ejecute en segundo plano (el análisis se ejecuta en el almacén de buzones y de carpetas públicas, por ejemplo la base de datos de Exchange). Microsoft Exchange Server decide si se ejecutará un análisis en segundo plano o no en función de varios factores, como la carga actual del sistema, el número de usuarios activos, etc. Si va a abrir un mensaje que no se ha analizado con la base de firmas de virus más actual, Microsoft Exchange Server envía el mensaje a ESET Mail Security para su análisis antes de abrirlo en el cliente de correo electrónico. Puede seleccionar la opción **Analizar solo mensajes con archivos adjuntos** y realizar el filtrado en función de la fecha y hora de recepción con las siguientes opciones de **Nivel de análisis**:

- **Todos los mensajes**
- **Mensajes recibidos en el último año**
- **Mensajes recibidos en los últimos 6 meses**
- **Mensajes recibidos en los últimos 3 meses**
- **Mensajes recibidos el último mes**
- **Mensajes recibidos la última semana**

El análisis en segundo plano puede afectar a la carga del sistema (el análisis se realiza cada vez que se actualiza la base de firmas de virus), por lo que le recomendamos que programe los análisis para que se ejecuten fuera de las horas de oficina. El análisis en segundo plano programado se puede configurar con una tarea especial de Tareas programadas o el Planificador. Cuando programe una tarea de análisis en segundo plano, puede definir la hora de inicio, el número de repeticiones y otros parámetros disponibles en Tareas programadas. Una vez que haya programado la tarea, esta aparecerá en la lista de tareas programadas y podrá modificar sus parámetros, eliminarla o desactivarla de forma temporal.

Al activar la opción **Analizar cuerpos de mensajes RTF**, se activa el análisis de los cuerpos de mensajes RTF. Estos mensajes pueden contener macrovirus.

NOTA: VSAPI no analiza los cuerpos de mensajes de texto sin formato.

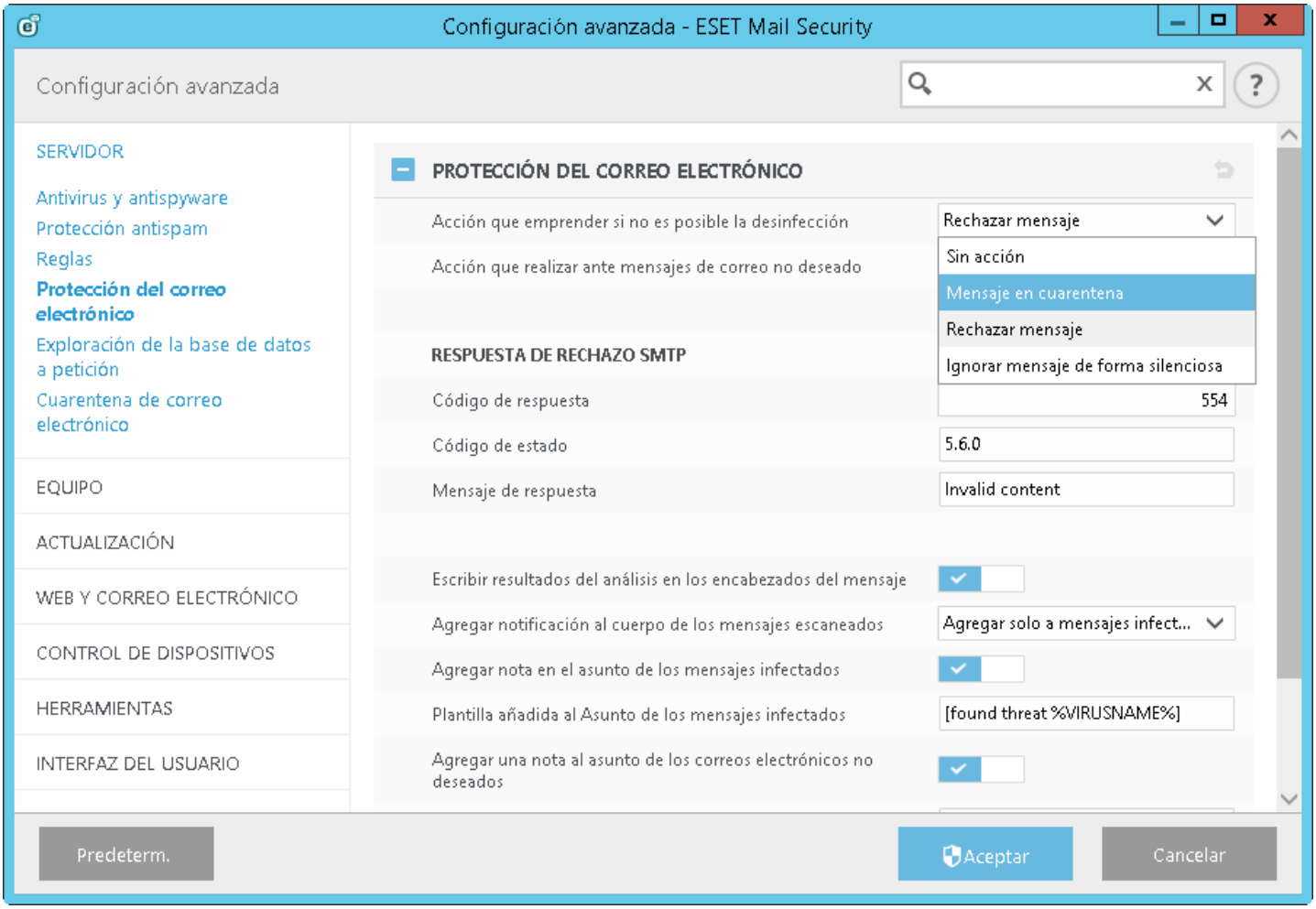
NOTA: Las carpetas públicas se tratan de la misma forma que los buzones, lo que significa que las carpetas públicas también se analizan.

5.1.7 Protección del correo electrónico

Los siguientes sistemas operativos tienen la opción **Protección del transporte del correo electrónico** disponible en **Configuración avanzada** > **Servidor**:

- Microsoft Exchange Server 2007 (servidor de Transporte perimetral o Concentrador de transporte)
- Microsoft Exchange Server 2007 (instalación de un solo servidor con varios roles)
- Microsoft Exchange Server 2010 (servidor de Transporte perimetral o Concentrador de transporte)
- Microsoft Exchange Server 2010 (instalación de un solo servidor con varios roles)
- Microsoft Exchange Server 2013 (rol de servidor de Transporte perimetral)
- Microsoft Exchange Server 2013 (instalación de un solo servidor con varios roles)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

Configuración de la protección del correo electrónico:



La acción antivirus de la capa de transporte puede configurarse en **Acción que emprender si no es posible la desinfección**:

- **Sin acción**: conservar los mensajes infectados que no pueden desinfectarse.
- **Poner mensaje en cuarentena**: envía al buzón de correo de cuarentena los mensajes infectados.
- **Rechazar mensaje**: rechaza los mensajes infectados.
- **Ignorar mensaje de forma silenciosa**: elimina los mensajes sin enviar NDR (Informe de no entrega).

La acción antispam en la capa de transporte se puede configurar en **Acción a emprender en mensajes no deseados**:

- **Sin acción**: conserva el mensaje aunque se marque como spam.
- **Poner mensaje en cuarentena**: envía los mensajes marcados como spam al buzón de correo de cuarentena.
- **Rechazar mensaje**: rechaza los mensajes marcados como spam.
- **Ignorar mensaje de forma silenciosa**: elimina los mensajes sin enviar NDR (Informe de no entrega).

Respuesta SMTP de rechazo: puede especificar valores de **Código de respuesta**, **Código de estado** y **Mensaje de respuesta** que definen la respuesta de denegación de SMTP temporal enviada al servidor SMTP si se rechaza un mensaje. El mensaje de respuesta se puede escribir con el formato siguiente:

Código de respuesta	Código de estado	Mensaje de respuesta
250	2.5.0	Aceptación de la acción del correo: completada
451	4.5.1	Se canceló la acción solicitada: error local al procesar
550	5.5.0	No se realizó la acción solicitada: el buzón de correo no está disponible

554	5.6.0	Contenido no válido

NOTA: en la configuración de respuestas SMTP de rechazo también puede utilizar variables del sistema.

Escribir resultados del análisis en los encabezados del mensaje: cuando esta opción está activada, los resultados del análisis se escriben en los encabezados del mensaje. Estos encabezados de mensaje comienzan por `X_ESET`, lo que hace que sean fáciles de reconocer (por ejemplo `X_EsetResult` o `X_ESET_Antispam`).

Agregar notificación al cuerpo de los mensajes escaneados ofrece tres opciones:
- No adjuntar a mensajes
- Agregar solo a mensajes infectados
- Agregar a todos los mensajes analizados (no se aplica a los mensajes internos)

Agregar nota en el asunto de los mensajes infectados: cuando esta opción está activada, <%PN%> agrega una etiqueta de notificación al asunto del correo electrónico con el valor definido en el campo de texto **Plantilla añadida al Asunto de los mensajes infectados** (de forma predeterminada, `[found threat %VIRUSNAME%]`). Esta modificación puede utilizarse para automatizar el filtrado de los mensajes infectados mediante el filtrado del correo electrónico que presenta un asunto concreto, usando por ejemplo reglas o en el cliente (si el cliente de correo electrónico admite esta opción), para colocar estos mensajes de correo electrónico en una carpeta independiente.

Agregar una nota al asunto de los correos electrónicos no deseados: cuando esta opción está activada, <%PN%> agrega una etiqueta de notificación al asunto del correo electrónico con el valor definido en el campo de texto **Plantilla añadida al asunto de los mensajes no deseados** (de forma predeterminada, `[SPAM]`). Esta modificación puede utilizarse para automatizar el filtrado del correo no deseado mediante el filtrado del correo electrónico que presenta un asunto concreto, usando por ejemplo reglas o en el cliente (si el cliente de correo electrónico admite esta opción), para colocar estos mensajes de correo electrónico en una carpeta independiente.

NOTA: también puede usar las variables del sistema al editar el texto que se añadirá al asunto.

5.1.7.1 Configuración avanzada

En esta sección puede modificar la configuración avanzada aplicada al agente de transporte:

- **Analizar también los mensajes procedentes de conexiones autenticadas o internas**: puede elegir el tipo de análisis a realizar en los mensajes recibidos de fuentes autenticadas o servidores locales. Se recomienda realizar el análisis de estos mensajes porque aumenta la protección, aunque este análisis será necesario si se utiliza el conector POP3 integrado de Microsoft SBS para recuperar mensajes de correo electrónico desde servidores de POP3 externos o servicios de correo electrónico (por ejemplo **Gmail.com**, **Outlook.com**, **Yahoo.com**, **gmx.dem**, etc.). Para obtener más información, consulte Protección antispam y conector POP3.

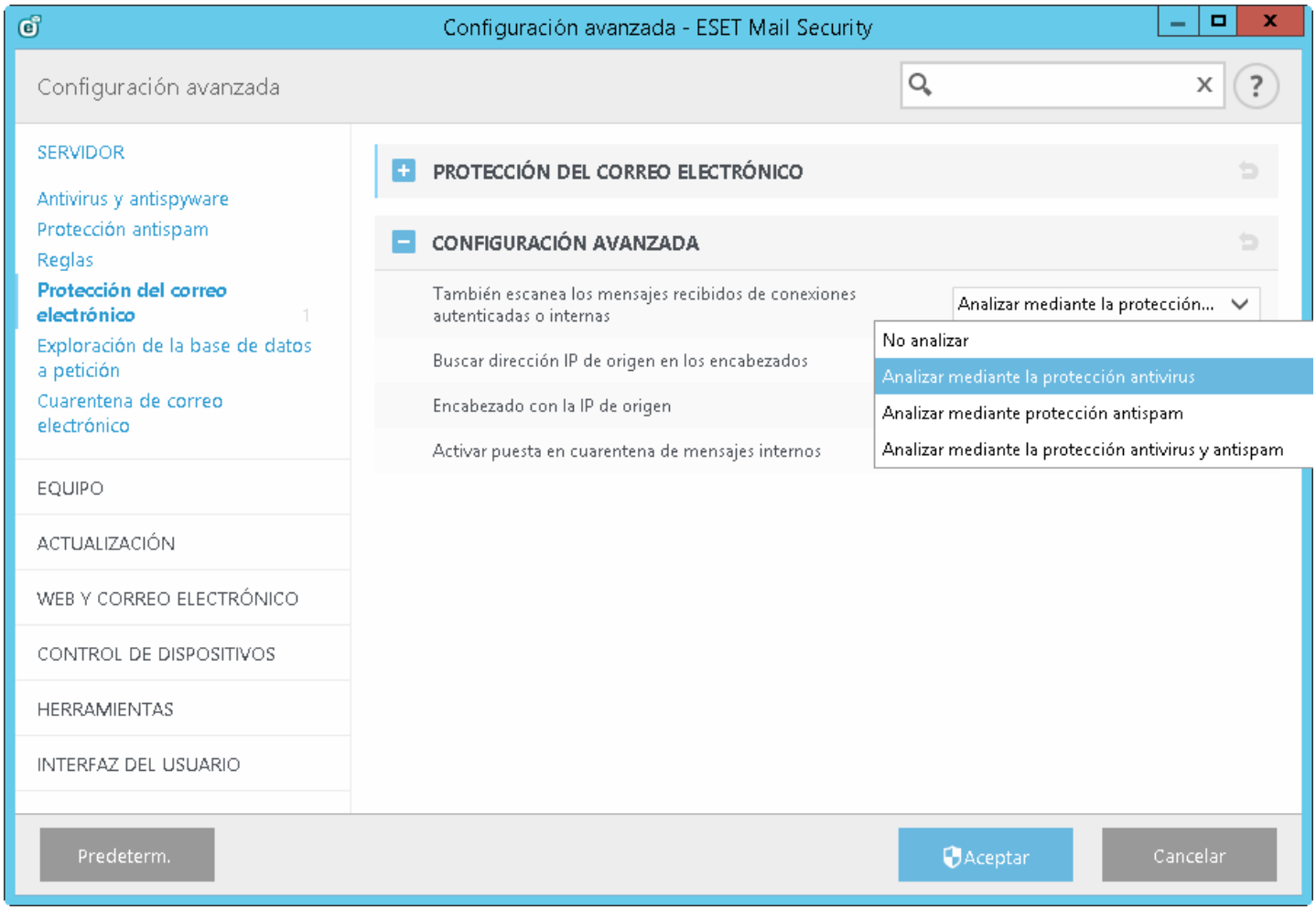
NOTA: los mensajes internos de Outlook de dentro de la organización se envían en formato TNEF (Transport Neutral Encapsulation Format). El formato TNEF no es compatible con el motor antispam. Por lo tanto, los correos electrónicos con formato TNEF internos no se analizarán en busca de correo no deseado ni siquiera si selecciona **Analizar mediante protección antispam** o **Analizar mediante la protección antivirus y antispam**.

- **Buscar dirección IP de origen en los encabezados**: si está activado, ESET Mail Security busca la dirección IP de origen en encabezados de mensajes para que los diferentes módulos de protección (antispam y otros) puedan utilizarla. Si su organización de Exchange está separada de Internet por un proxy, puerta de enlace o servidor de transporte perimetral, los mensajes de correo electrónico parecen llegar desde una dirección IP única (normalmente una dirección interna). Es habitual que en el servidor exterior (por ejemplo, transporte perimetral en DMZ), donde se conoce la dirección IP de los remitentes, esta dirección IP se escriba en los encabezados de mensajes de correo electrónico recibidos. El valor especificado en el campo **Encabezado con la IP de origen** siguiente es el encabezado que ESET Mail Security busca en los encabezados de mensajes.

- **Encabezado con la IP de origen**: es el encabezado que ESET Mail Security busca en los encabezados de mensajes. El valor predeterminado es **IP de origen X**, aunque si se utilizan herramientas de terceros o personalizadas que utilicen encabezados diferentes, cámbielo al valor correspondiente.

- **Activar puesta en cuarentena de mensajes internos**: cuando esté activado, se pondrán en cuarentena los mensajes internos. Normalmente no es necesario poner en cuarentena los mensajes internos, pero si lo necesita,

puede activar la cuarentena.



5.1.8 Análisis de la base de datos a petición

Lista de sistemas que tienen la opción **Análisis de la base de datos a petición** disponible:

- Microsoft Exchange Server 2007 (servidor de buzones o servidor de Concentrador de transporte)
- Microsoft Exchange Server 2007 (instalación de un solo servidor con varios roles)
- Microsoft Exchange Server 2010 (servidor de buzones o servidor de Concentrador de transporte)
- Microsoft Exchange Server 2010 (instalación de un solo servidor con varios roles)
- Microsoft Exchange Server 2013 (rol de servidor de buzones)
- Microsoft Exchange Server 2013 (instalación de un solo servidor con varios roles)
- Windows Small Business Server 2008
- Windows Small Business Server 2011

NOTA: Si está ejecutando Microsoft Exchange Server 2007 o 2010, puede optar entre Protección de la base de datos de buzones y Análisis de la base de datos a petición. Sin embargo, solo uno de estos dos tipos de protección puede estar activo al mismo tiempo. Si opta por usar el Análisis de la base de datos a petición, tendrá que desactivar la integración de la Protección de la base de datos de buzones en Configuración avanzada, dentro de la opción Servidor. De lo contrario, el Análisis de la base de datos a petición no estará disponible.

Configuración del análisis de la base de datos a petición:

Dirección del host: nombre o dirección IP del servidor en el que se ejecuta EWS (Exchange Web Services).

Nombre de usuario: especifique las credenciales de un usuario que tenga acceso adecuado a EWS (Exchange Web Services).

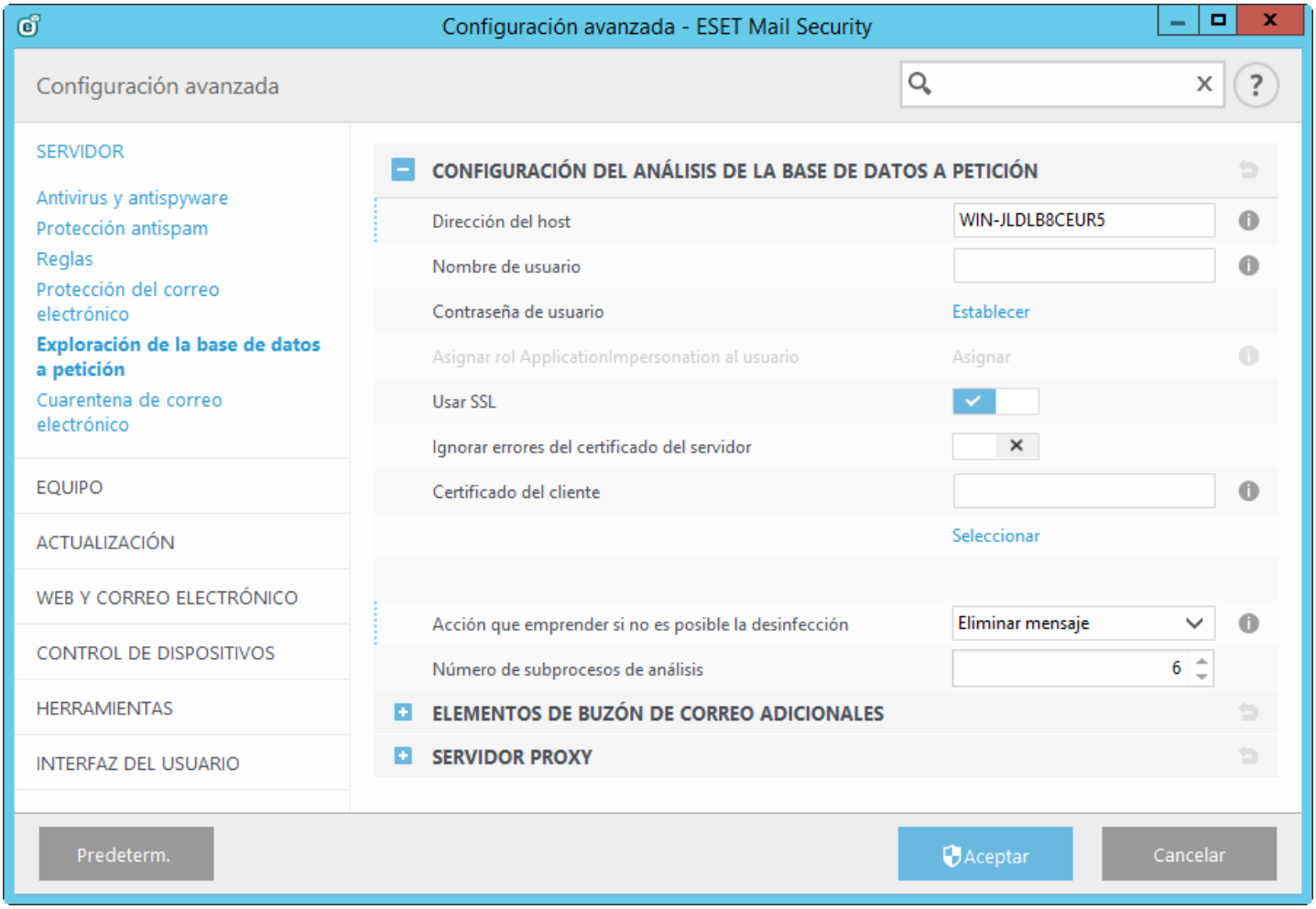
Contraseña del usuario: haga clic en **Definir** junto a **Contraseña del usuario** y escriba la contraseña de esta cuenta de usuario.

Asignar rol ApplicationImpersonation al usuario: si esta opción está atenuada, tendrá que especificar primero **Nombre de usuario**. Haga clic en **Asignar** para asignar automáticamente el rol ApplicationImpersonation al usuario seleccionado. También puede asignar el rol ApplicationImpersonation manualmente a una cuenta de usuario. Para obtener más información, consulte Detalles de la cuenta de análisis de la base de datos.

Usar SSL: se debe activar si EWS (Exchange Web Services) está configurado como **Requerir SSL** en IIS. Si SSL está activado, el certificado de Exchange Server debe importarse en sistema mediante ESET Mail Security (en caso de que los roles de Exchange Server se encuentren en servidores distintos). La configuración de EWS puede encontrarse en IIS en la ruta *Sitios/Sitio Web predeterminado/EWS/Configuración de SSL*.

NOTA: desactive la opción **Usar SSL** solo si tiene EWS configurado en IIS para no Requerir SSL.

Certificado del cliente: solo se debe configurar cuando Exchange Web Services requiere certificados del cliente. **Seleccionar** le permite seleccionar cualquiera de los certificados.



Acción que emprender si no es posible la desinfección: este campo de acción le permite **bloquear** el contenido infectado.

Sin acciones: no realiza ninguna acción en el contenido infectado del mensaje.
Mover mensaje a la papelera: no es compatible con los elementos de la carpeta pública. Puede usar **Eliminar objeto** y se aplicará esta acción en su lugar.
Eliminar objeto: contenido infectado del mensaje.
Eliminar mensaje: elimina todo el mensaje, incluido el contenido infectado.
Reemplazar objeto con información de la acción: elimina un objeto y coloca información sobre la acción que se realizó con este objeto.

5.1.8.1 Elementos de buzón de correo adicionales

La configuración del módulo de análisis de la base de datos a petición le permite activar o desactivar el análisis de otros tipos de elementos de buzón de correo:

- Analizar calendario
- Analizar tareas
- Analizar contactos
- Analizar diario

NOTA: si sufre problemas de rendimiento, puede desactivar el análisis de estos elementos. Cuando estos elementos estén activados, los análisis tardarán más en completarse.

5.1.8.2 Servidor Proxy

Si utiliza un servidor proxy entre la instancia de Exchange Server con el rol CAS y la instancia de Exchange Server en la que está instalado ESET Mail Security, especifique los parámetros de su servidor proxy. Esto resulta necesario porque ESET Mail Security se conecta a la API de EWS (Exchange Web Services) a través de HTTP/HTTPS. De lo contrario, el Análisis de la base de datos a petición no funcionará.

Servidor proxy: introduzca la dirección IP o el nombre del servidor proxy que desea utilizar.

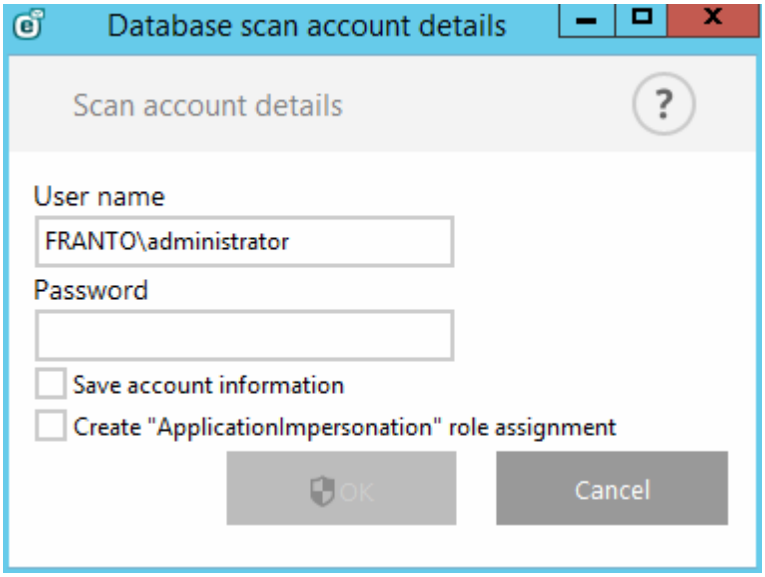
Puerto: introduzca el número de puerto del servidor proxy.

Nombre de usuario, contraseña: si su servidor proxy requiere autenticación, introduzca las credenciales.

5.1.8.3 Detalles de la cuenta de análisis de la base de datos

Este cuadro de diálogo aparece si no ha especificado un nombre de usuario y una contraseña para **Análisis de la base de datos** en **Configuración avanzada**. Especifique las credenciales del usuario que dispone de acceso a EWS (Exchange Web Services) en esta ventana emergente, y haga clic en **Aceptar**. Otra opción es acceder a la **Configuración avanzada** pulsando **F5** y accediendo a **Servidor** > Análisis de la base de datos a petición. Escriba su **Nombre de usuario**, haga clic en **Establecer**, escriba la contraseña de esta cuenta de usuario y, a continuación, haga clic en Aceptar.

- Puede seleccionar **Guardar información de la cuenta** para guardar la configuración de la cuenta y no tener que introducir dicha información cada vez que ejecute un análisis de la base de datos a petición.
- Si una cuenta de usuario no dispone del acceso adecuado a EWS, puede seleccionar **Crear asignación del rol "ApplicationImpersonation"** para asignar este rol a una cuenta. También puede asignar la función ApplicationImpersonation de forma manual, consulte la siguiente nota para obtener más información.



IMPORTANTE: la cuenta de análisis debe tener derechos **ApplicationImpersonation** asignados para que el motor de análisis analice los buzones de correo de usuarios de las bases de datos de buzones de Exchange. En Exchange Server 2010 o versiones más recientes, se recomienda encarecidamente configurar la política de aceleración en la

cuenta de análisis con el fin de evitar un exceso de solicitudes de operaciones por parte de ESET Mail Security. De lo contrario, su Exchange Server podría provocar que algunas de las solicitudes de operaciones agotaran su tiempo de espera.

NOTA: si desea asignar la función ApplicationImpersonation a una cuenta de usuario de forma manual, puede utilizar los siguientes comandos (sustituya `usuario-ESET` por un nombre de cuenta real de su sistema):

Exchange Server 2007

```
Get-ClientAccessServer | Add-AdPermission -User usuario-ESET -ExtendedRights ms-Exch-EPI-Impersonatio

Get-MailboxDatabase | Add-AdPermission -User usuario-ESET -ExtendedRights ms-Exch-EPI-May-Impersonate
```

Exchange Server 2010

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation
-User:usuario-ESET
```

Su aplicación puede tardar unos instantes

```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSFindCountLimit $null -EWSFastSearchTimeoutInSeco

Set-ThrottlingPolicyAssociation -Identity usuario-ESET -ThrottlingPolicy ESET-ThrottlingPolicy
```

Exchange Server 2013

```
New-ManagementRoleAssignment -Name:ESET-ApplicationImpersonation -Role:ApplicationImpersonation
-User:usuario-ESET
```

Su aplicación puede tardar unos instantes

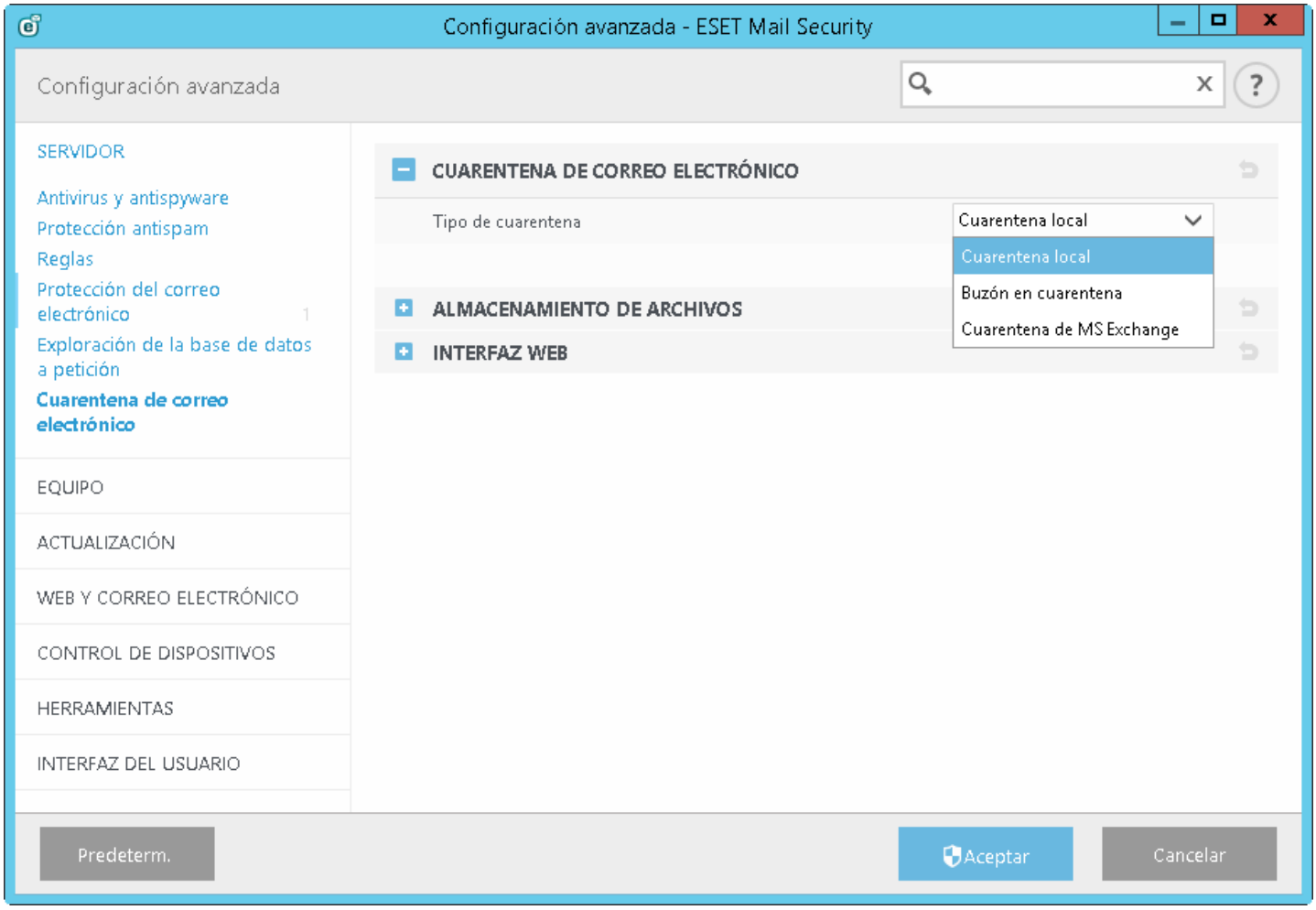
```
New-ThrottlingPolicy -Name ESET-ThrottlingPolicy -EWSMaxConcurrency Unlimited -EwsCutoffBalance Unlim

Set-ThrottlingPolicyAssociation -Identity usuario-ESET -ThrottlingPolicy ESET-ThrottlingPolicy
```

5.1.9 Cuarentena de correo electrónico

El administrador de la cuarentena de correo electrónico está disponible para los tres tipos de cuarentena:

- Cuarentena local
- Buzón en cuarentena
- Cuarentena de MS Exchange



Puede ver el contenido de la cuarentena de correo electrónico en el Administrador de la cuarentena de correo electrónico de todos los tipos de cuarentena. Además, la cuarentena local también puede visualizarse en la Interfaz web de la cuarentena de correo.

5.1.9.1 Cuarentena local

La Cuarentena local utiliza el sistema de archivos local para almacenar los correos electrónicos puestos en cuarentena y una base de datos de SQLite como índice. Los archivos de correo electrónico puestos en cuarentena y los archivos de la base de datos almacenados se cifran por motivos de seguridad. Estos archivos se encuentran en `C:\ProgramData\ESET\ESET Mail Security\MailQuarantine` (en Windows Server 2008 y 2012) o `C:\Documents and Settings\All Users\Application Data\ESET\ESET Mail Security\MailQuarantine` (en Windows Server 2003).

NOTA: si desea almacenar los archivos en cuarentena en un disco que no sea la unidad predeterminada, es decir, la unidad `C:`, tendrá que cambiar la **Carpeta de datos** a su ruta preferida durante la instalación de ESET Mail Security.

Características de la cuarentena local:

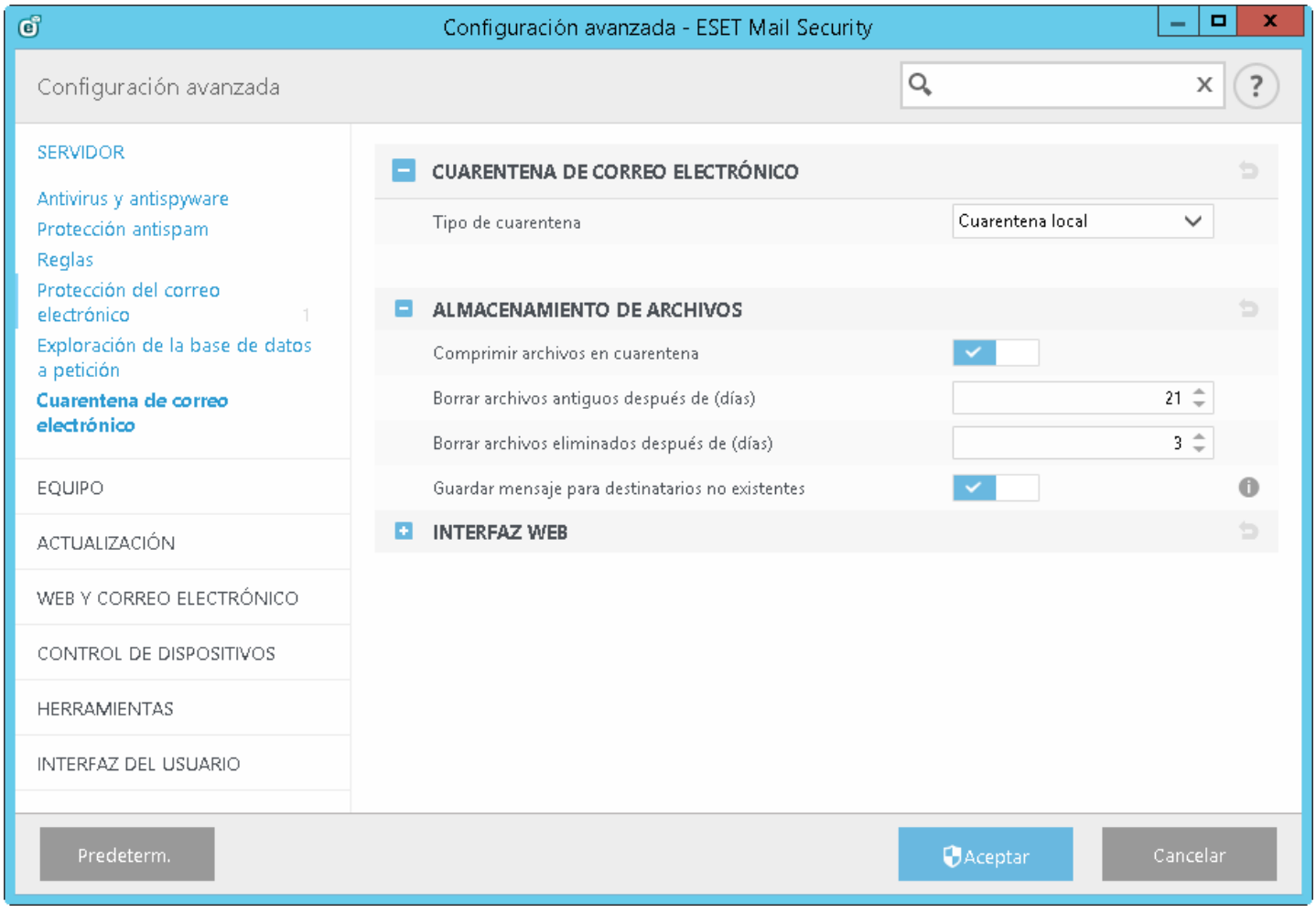
- Los mensajes de correo electrónico no deseados y en cuarentena se almacenarán en un sistema de archivos local, lo que significa que no se incluirán en la base de datos de buzones de Exchange.
- Cifrado y compresión de los archivos de correo electrónico almacenados de forma local.
- Interfaz web de la Cuarentena de correo electrónico como alternativa al Administrador de la cuarentena de correo electrónico.
- Los informes de la cuarentena se pueden enviar a una dirección de correo electrónico especificada por medio de una tarea programada.
- Los archivos de correo electrónico puestos en cuarentena eliminados de la ventana de cuarentena (después de 21 días, de forma predeterminada), se siguen almacenando en un sistema de archivos (hasta que la eliminación automática se produce después del número de días especificado).
- Eliminación automática de los archivos de correo electrónico antiguos (después de 3 días, de forma predeterminada). Para obtener más información, consulte la configuración del Almacenamiento de archivos.
- Puede restaurar los archivos de correo electrónico puestos en cuarentena eliminados con eShell (suponiendo que aún no se han eliminado del sistema de archivos).

NOTA: la desventaja de la cuarentena local es que si ejecuta varios servidores de ESET Mail Security con la función Servidor concentrador de transporte, tendrá que gestionar la cuarentena local de cada servidor por separado. Cuantos más servidores tenga, más cuarentenas tendrá que gestionar.

Puede inspeccionar los mensajes de correo electrónico puestos en cuarentena y optar por **eliminar** o **liberar** los que quiera. Para ver y gestionar los mensajes de correo electrónico puestos en cuarentena a nivel local, puede usar el Administrador de la cuarentena de correo electrónico desde la interfaz gráfica de usuario principal o la Interfaz web de la cuarentena de correo electrónico.

5.1.9.1.1 Almacenamiento de archivos

En esta sección puede cambiar la configuración del almacenamiento de archivos utilizado por la cuarentena local.



Comprimir archivos en cuarentena: los archivos en cuarentena comprimidos ocupan menos espacio en disco, pero si opta por no comprimir los archivos, utilice el conmutador para desactivar la compresión.

Borrar archivos antiguos después de (días): cuando los mensajes llegan al número de días especificado, se eliminan de la ventana de cuarentena. Sin embargo, los archivos no se eliminarán del disco durante la cantidad de días específica en **Borrar archivos eliminados después de (días)**. Como los archivos no se eliminan del sistema de archivos, es posible recuperarlos con eShell.

Borrar archivos eliminados después de (días): elimina los archivos del disco después del número de días especificado, no es posible recuperarlos después de eliminarlos (a menos que cuente con una solución de copia de seguridad del sistema de archivos).

Guardar mensaje para destinatarios no existentes: normalmente, los mensajes de spam se envían a destinatarios aleatorios de un dominio determinado, en un intento de que el mensaje llegue a un destinatario real. Los mensajes enviados a usuarios que no existen en un Active Directory se almacenan, de forma predeterminada, en la cuarentena local. No obstante, puede desactivar esta opción y los mensajes enviados a destinatarios no existentes no se almacenarán. De esta forma, la cuarentena local no estará saturada de muchos mensajes de spam de este mismo tipo. De esta forma se ahorra espacio en disco.

5.1.9.1.2 Interfaz web

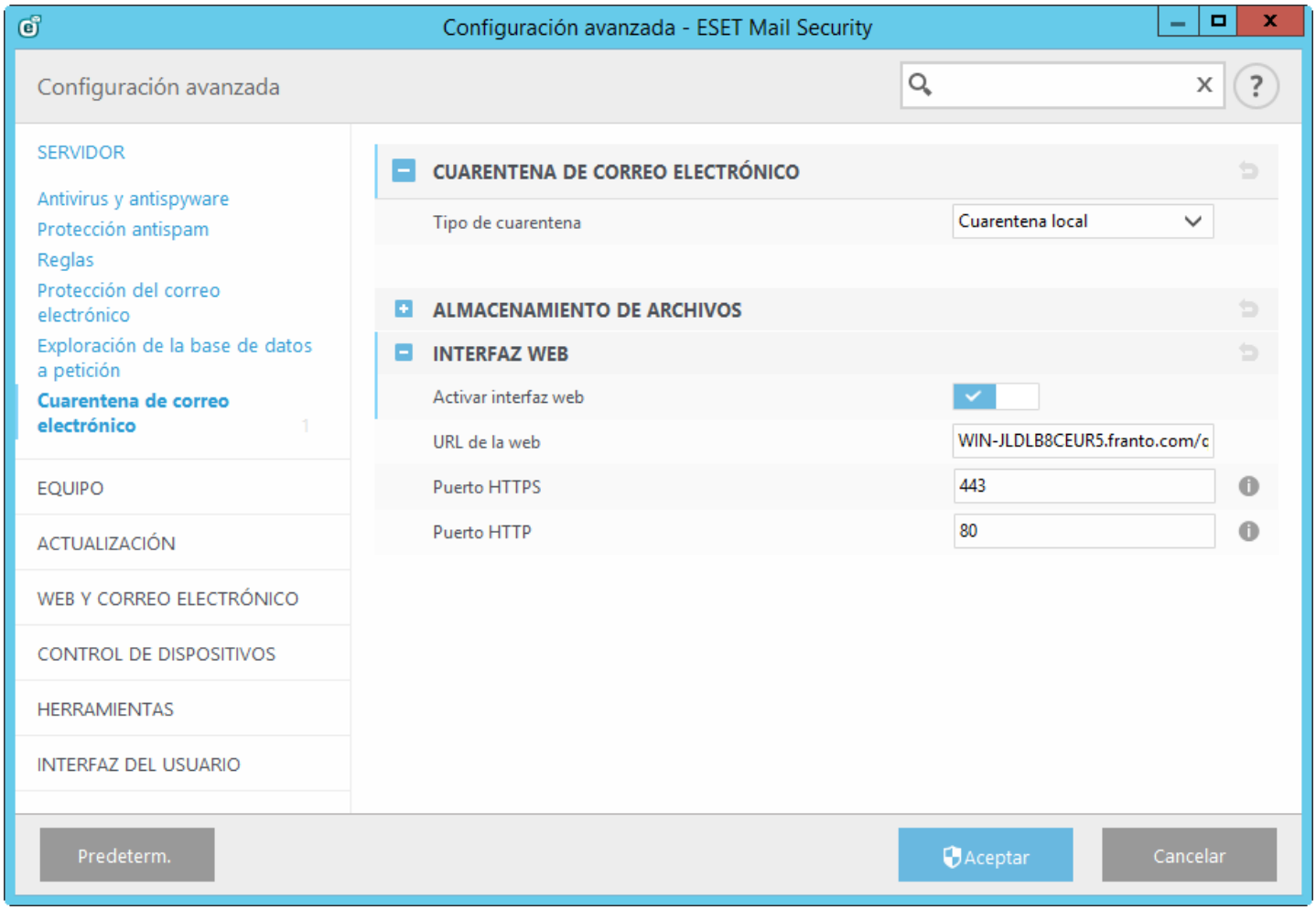
La interfaz web de la cuarentena de correo es una alternativa al Administrador de la cuarentena de correo electrónico que solo está disponible para la Cuarentena local.

NOTA: la interfaz web de la cuarentena de correo no está disponible en un servidor con rol de servidor de transporte perimetral. El motivo es que Active Directory no está accesible para autenticación.

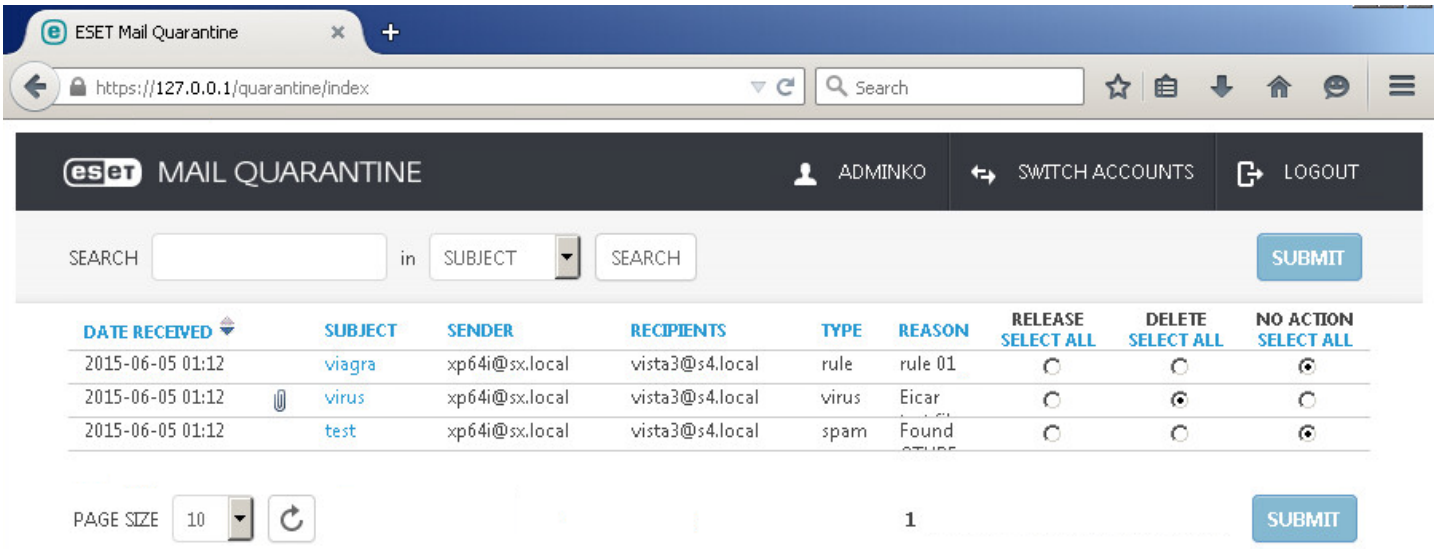
La interfaz web de la cuarentena de correo electrónico le permite ver el estado de la cuarentena de correo electrónico. Además, le permite gestionar los objetos de correo electrónico que están en la cuarentena. A esta interfaz web se puede acceder desde los vínculos de los informes de la cuarentena, y también introduciendo directamente una URL en su navegador web. Para acceder a la interfaz web de la cuarentena de correo electrónico se debe autenticar con las credenciales de dominio. Internet Explorer autenticará automáticamente a un usuario de dominio; el certificado de la página web debe ser válido, el inicio de sesión automático debe estar activado en Internet Explorer y debe agregar el sitio web de la cuarentena de correo electrónico a los sitios de la intranet local.

El conmutador **Activar interfaz web** le permite activar o desactivar la interfaz web.

URL web: esta es la URL en la que estará disponible la interfaz web de la Cuarentena de correo electrónico. De forma predeterminada, es el FQDN del servidor junto con `/quarantine` (p. ej. `mailserver.company.com/quarantine`).
Puerto HTTPS: el número de puerto predeterminado es el 443, aunque puede cambiarlo si lo desea.
Puerto HTTP: el número de puerto predeterminado es el 80, aunque puede cambiarlo si lo desea.

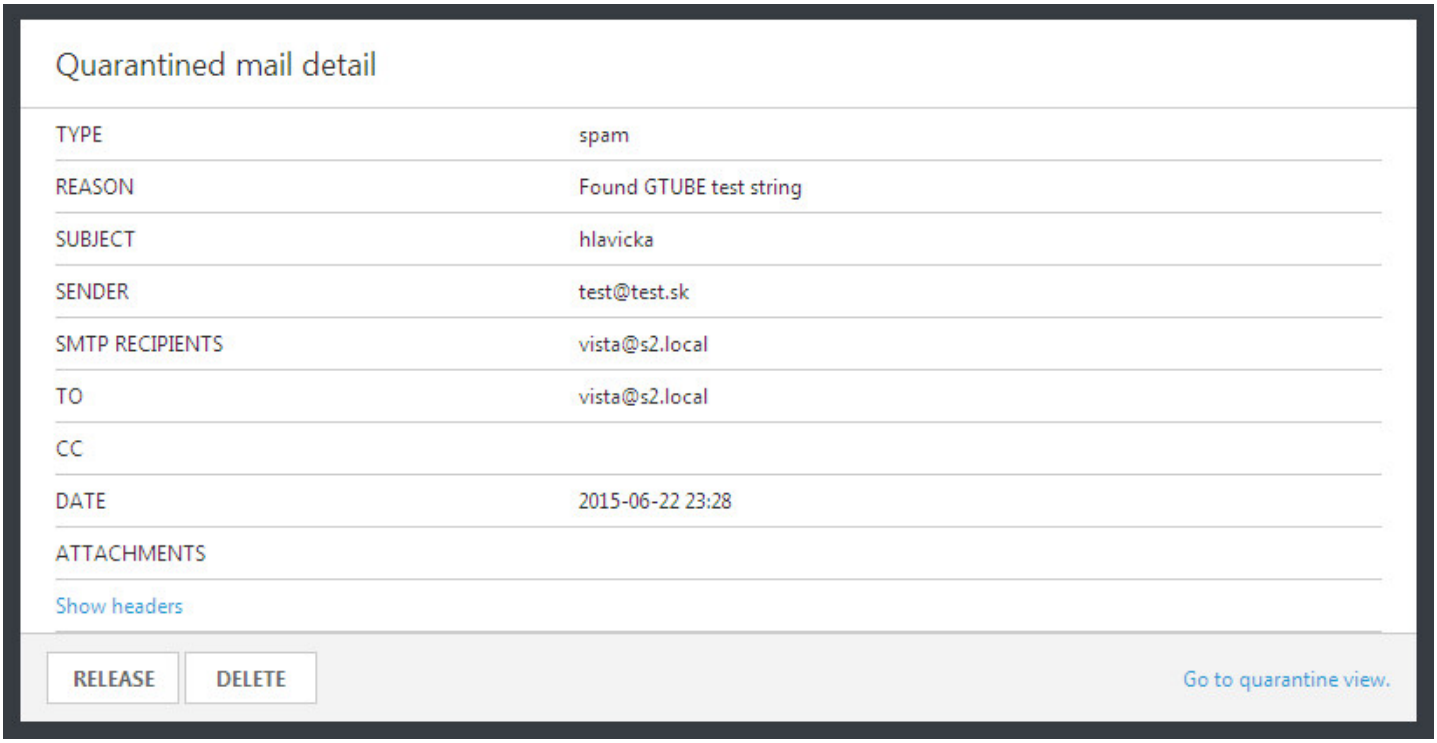


Para acceder a la interfaz web de la Cuarentena de correo electrónico, abra el navegador web y utilice la URL especificada en **Configuración avanzada** > **Servidor** > **Cuarentena de correo electrónico** > **Interfaz web** > **URL web**.

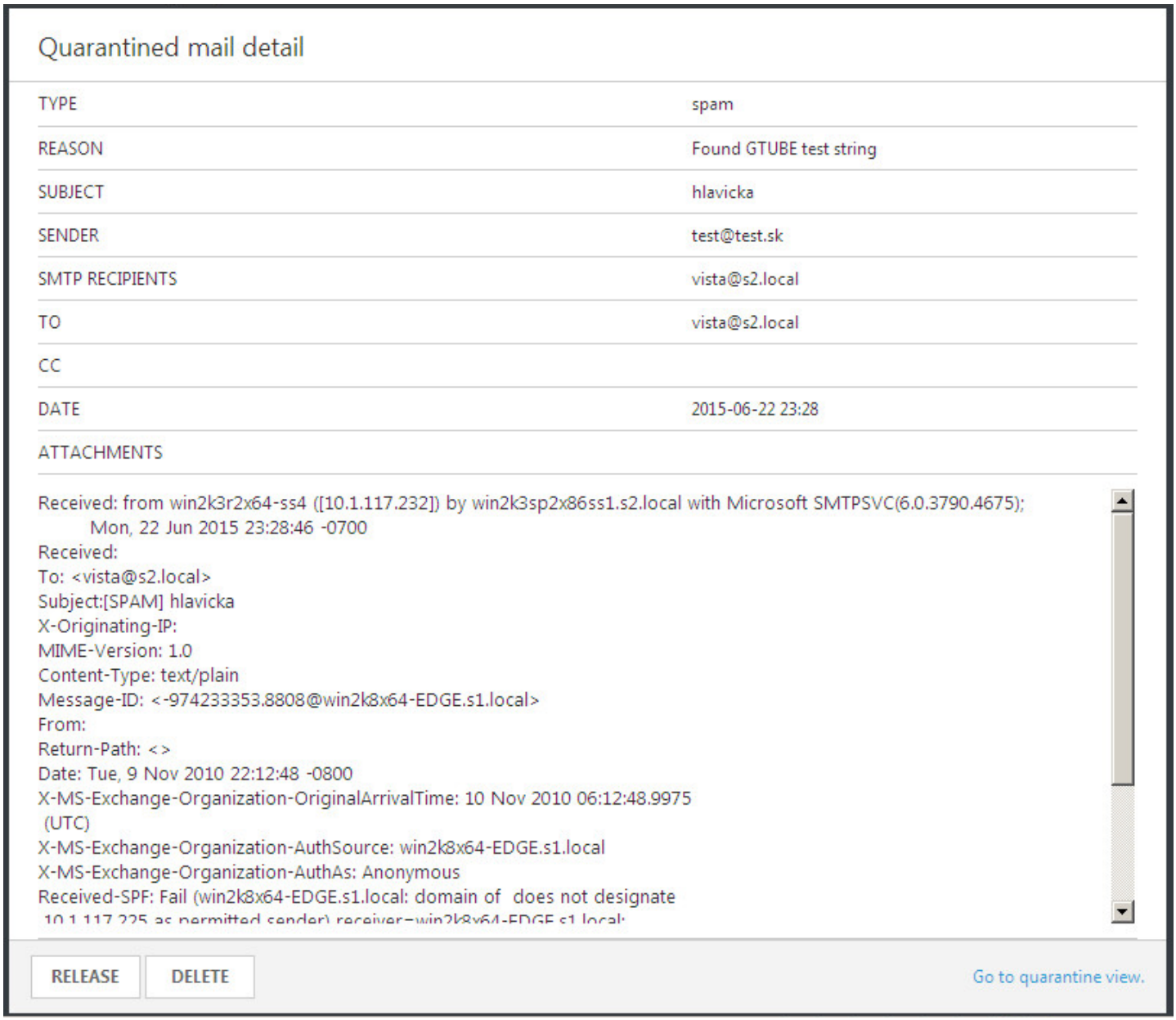


Liberar: libera el correo electrónico hacia sus destinatarios originales utilizando el directorio de retransmisión, y lo elimina de la cuarentena. Haga clic en **Enviar** para confirmar la acción.
Eliminar: elimina el elemento de la cuarentena. Haga clic en **Enviar** para confirmar la acción.

Cuando hace clic en **Asunto**, se abre una ventana emergente con detalles sobre el correo electrónico puesto en cuarentena, con información de **Tipo**, **Motivo**, **Remitente**, **Fecha**, **Archivos adjuntos**, etc.

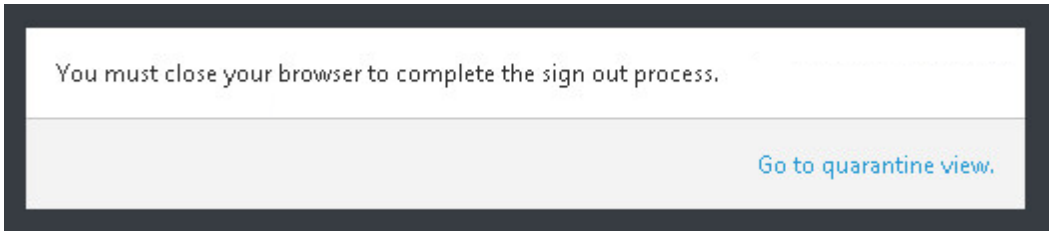


Haga clic en **Encabezados** para revisar el encabezado del correo electrónico puesto en cuarentena.



Si lo desea, haga clic en **Liberar** o **Eliminar** para realizar una acción con un mensaje de correo electrónico puesto en cuarentena.

NOTA: debe cerrar la ventana del navegador para cerrar por completo la sesión de la interfaz web de la cuarentena de correo electrónico. De lo contrario, haga clic en **Ir a la vista de cuarentena** para volver a la pantalla anterior.



IMPORTANTE: si tiene problemas a la hora de acceder a la interfaz web de la cuarentena de correo electrónico desde su navegador o recibe el error `HTTP Error 403.4 - Forbidden` o similar, compruebe qué tipo de cuarentena se encuentra seleccionado, y asegúrese de que sea la **Cuarentena local** y de que la opción **Activar interfaz web** se encuentre activada.

5.1.9.2 Buzón en cuarentena y cuarentena de MS Exchange

Si opta por no usar la Cuarentena local tiene dos opciones: el **Buzón en cuarentena** o la **Cuarentena de MS Exchange**. Elija la opción que elija, tendrá que crear un usuario dedicado con buzón (por ejemplo cuarentena_principal@empresa.com) que posteriormente se utilizará para almacenar los mensajes de correo electrónico puestos en cuarentena. El Administrador de la cuarentena de correo electrónico también utilizará este usuario y este buzón para ver y gestionar los elementos de la cuarentena. Tendrá que especificar los detalles de la cuenta de este usuario en la Configuración del administrador de la cuarentena.

IMPORTANTE: no se recomienda usar la cuenta de usuario Administrador como buzón en cuarentena.

NOTA: la **Cuarentena de MS Exchange** no está disponible en Microsoft Exchange 2003, solo la **Cuarentena local** y el **Buzón en cuarentena**.

- Cuando seleccione la **Cuarentena de MS Exchange**, ESET Mail Security utilizará el **Sistema de cuarentena de Microsoft Exchange** (esto se aplica a Microsoft Exchange Server 2007 y versiones más recientes). En este caso, el mecanismo interno de Exchange se utiliza para almacenar los mensajes potencialmente infectados y de correo no deseado.

NOTA: de forma predeterminada, la cuarentena interna no está activada en Exchange. Para activarla, abra la Consola de administración de Exchange y escriba el comando siguiente (sustituya `nombre@dominio.com` por una dirección real de su buzón de correo dedicado):

```
Set-ContentFilterConfig -QuarantineMailbox nombre@dominio.com
```

- Cuando seleccione el **Buzón en cuarentena** tendrá que especificar la dirección de cuarentena del mensaje (por ejemplo cuarentena_principal@empresa.com).

NOTA: la ventaja del buzón en cuarentena y de la cuarentena de MS Exchange con respecto a la cuarentena local es que los elementos de la cuarentena de correo electrónico se gestionan desde un solo lugar, independientemente del número de servidores que tengan la función Servidor concentrador de transporte. Sin embargo, el buzón en cuarentena y la cuarentena de MS Exchange presentan una desventaja, y es que los mensajes de correo no deseado y en cuarentena se almacenan en las bases de datos de buzones de Exchange, y solo el administrador puede gestionar la cuarentena de correo electrónico.

5.1.9.2.1 Configuración del administrador de la cuarentena

Dirección del host: aparecerá automáticamente si su Exchange Server con rol CAS está presente a nivel local. De lo contrario, si el rol CAS no está presente en el mismo servidor en el que está instalado ESET Mail Security pero puede encontrarse dentro del AD, la dirección del host aparecerá automáticamente. Si no aparece, puede escribir el nombre del host de forma manual. La detección automática no funcionará con el rol Servidor de transporte perimetral.

NOTA: no se admite la dirección IP, debe usar el nombre de host del servidor CAS.

Nombre de usuario: cuenta de usuario de cuarentena dedicada que ha creado para almacenar los mensajes puestos en cuarentena (o una cuenta que tiene acceso a este buzón mediante la delegación de acceso). En un rol de Servidor de transporte perimetral que no forma parte del dominio, es necesario utilizar la dirección de correo electrónico al completo (por ejemplo cuarentena_principal@empresa.com).

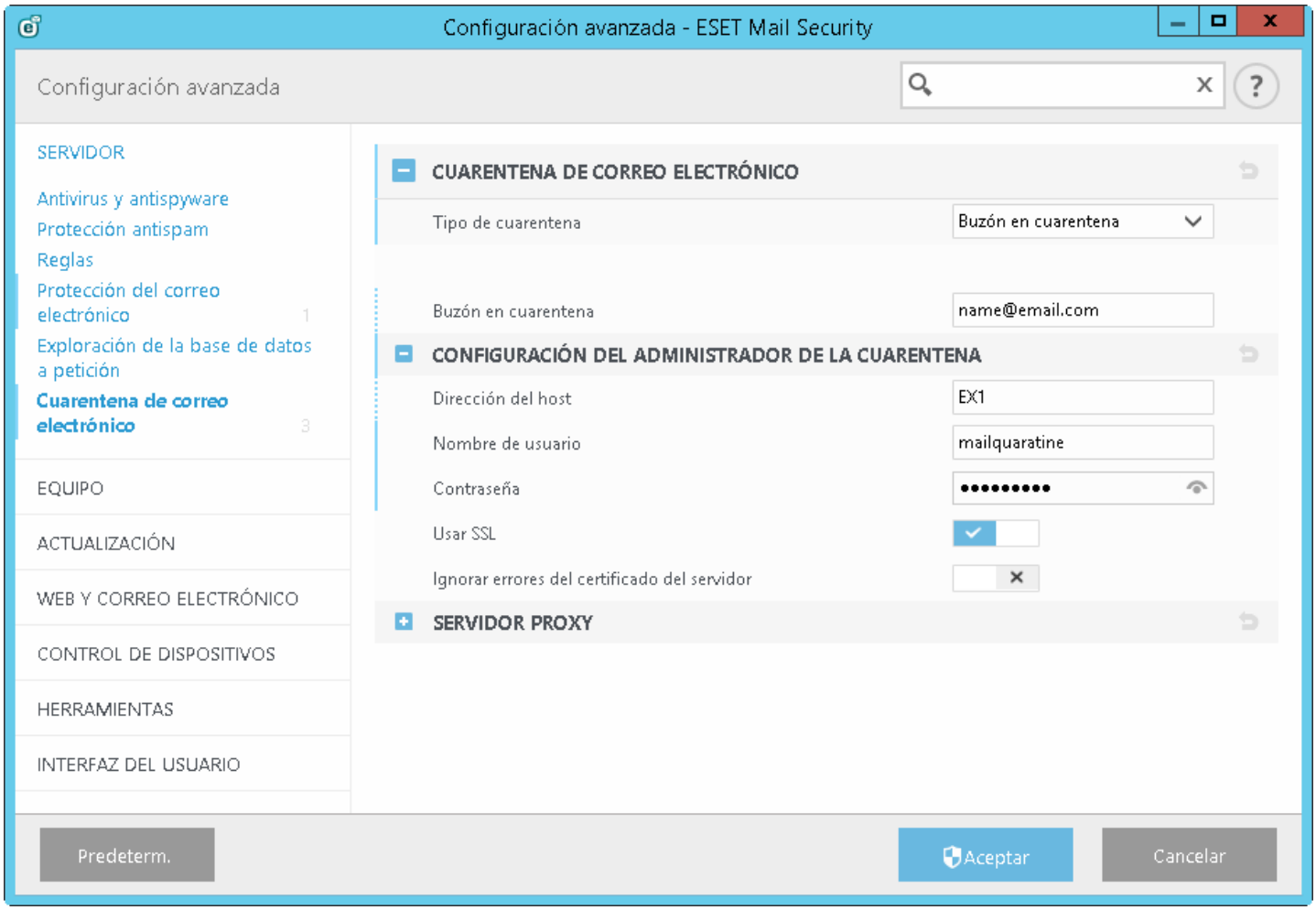
Contraseña: escriba la contraseña de su cuenta de cuarentena.

Usar SSL: se debe activar si EWS (Exchange Web Services) está configurado como **Requerir SSL** en IIS. Si SSL está activado, el certificado de Exchange Server debe importarse en sistema mediante ESET Mail Security (en caso de que los roles de Exchange Server se encuentren en servidores distintos). La configuración de EWS puede encontrarse en IIS en la ruta *Sitios/Sitio Web predeterminado/EWS/Configuración de SSL*.

NOTA: desactive la opción **Usar SSL** solo si tiene EWS configurado en IIS para no Requerir SSL.

Ignorar errores del certificado del servidor: ignora los siguientes estados: autofirmado, nombre incorrecto en el

certificado, uso erróneo, caducado.



5.1.9.2.2 Servidor proxy

Si utiliza un servidor proxy entre la instancia de Exchange Server con el rol CAS y la instancia de Exchange Server en la que está instalado ESET Mail Security, especifique los parámetros de su servidor proxy. Esto resulta necesario porque ESET Mail Security se conecta a la API de EWS (Exchange Web Services) a través de HTTP/HTTPS. De lo contrario, el buzón en cuarentena y la cuarentena de MS Exchange no funcionarán.

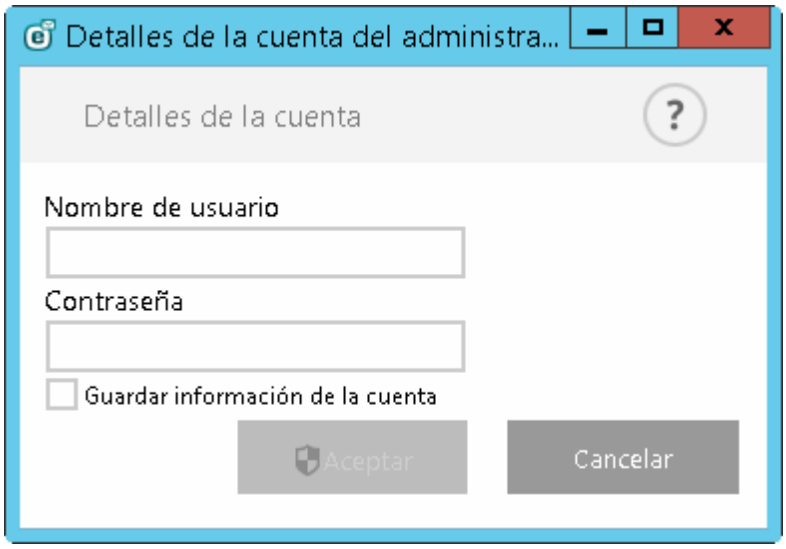
Servidor proxy: introduzca la dirección IP o el nombre del servidor proxy que desea utilizar.

Puerto: introduzca el número de puerto del servidor proxy.

Nombre de usuario, contraseña: si su servidor proxy requiere autenticación, introduzca las credenciales.

5.1.9.3 Detalles de la cuenta del administrador de la cuarentena

Este cuadro de diálogo aparecerá si no configura una cuenta para sus **Detalles del administrador de la cuarentena**. Especifique las credenciales del usuario que tiene acceso al **Buzón en cuarentena** y haga clic en **Aceptar**. También puede pulsar F5 para acceder a la **Configuración avanzada** y dirigirse a **Servidor** > **Cuarentena de correo electrónico** > Configuración del administrador de la cuarentena. Escriba el **Nombre de usuario** y la **Contraseña** de su buzón de correo de cuarentena.



Puede seleccionar **Guardar información de la cuenta** para guardar la configuración de la cuenta y usarla en un futuro al acceder al Administrador de la cuarentena.

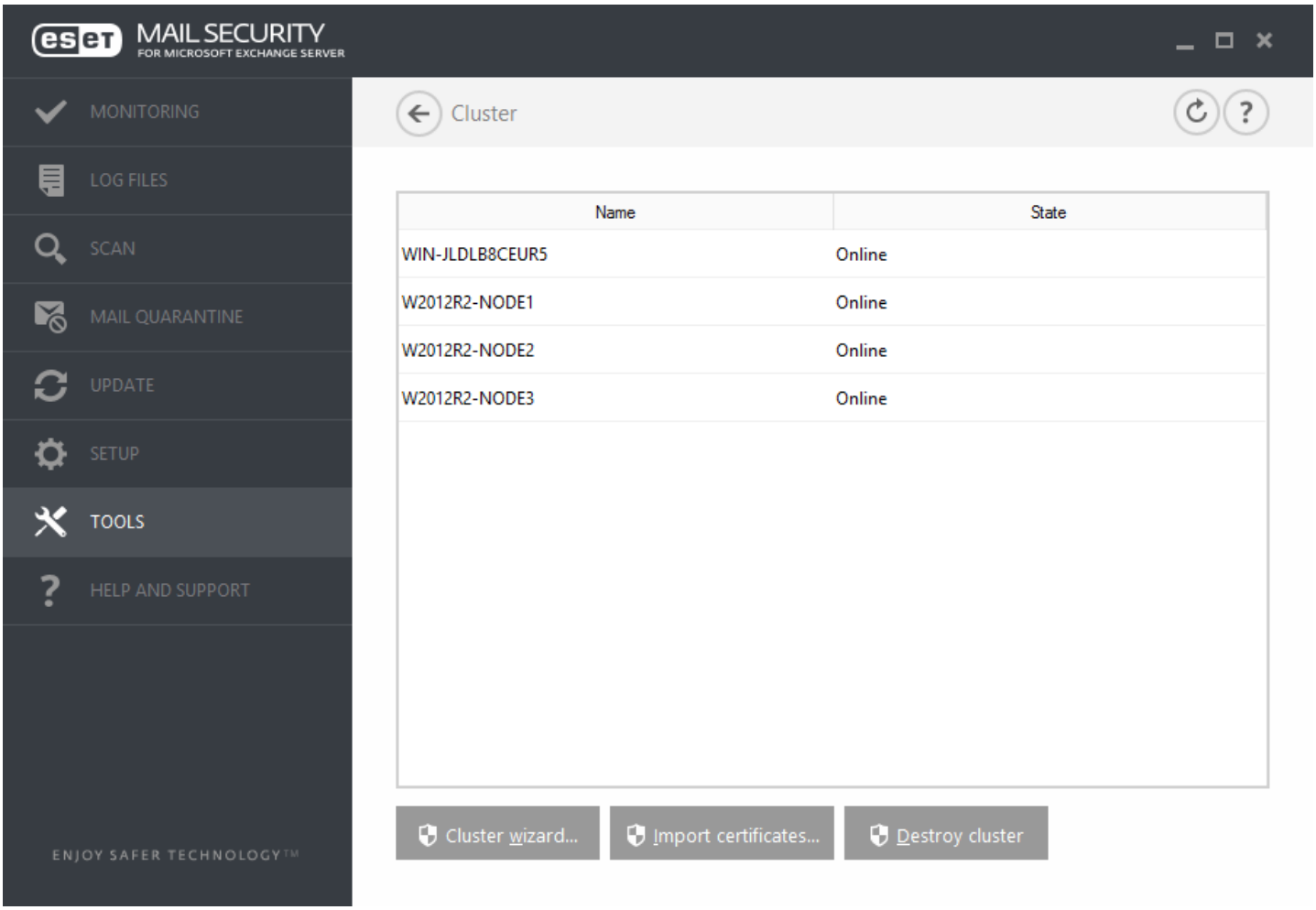
5.1.10 Clúster

El **Clúster de ESET** es una infraestructura de comunicación P2P de la gama de productos ESET para Microsoft Windows Server.

Esta infraestructura permite que los productos de servidor de ESET se comuniquen e intercambien datos como, por ejemplo, configuraciones y notificaciones, además de sincronizar los datos necesarios para el correcto funcionamiento de un grupo de instancias del producto. Un ejemplo de este tipo de grupo es un grupo de nodos de un clúster de conmutación por error de Windows o un clúster de equilibrio de carga de red (NLB) con un producto ESET instalado en el que es necesario que el producto tenga la misma configuración en todo el clúster. Clúster de ESET garantiza esta coherencia entre instancias.

NOTA: los ajustes de la interfaz de usuario no se sincronizan entre los nodos del Clúster de ESET.

A la página de estado de Clúster de ESET se accede desde el menú principal, con la ruta **Herramientas** > **Clúster**; cuando está correctamente configurado, la apariencia de la página de estado debe ser la siguiente:



Para configurar el Clúster de ESET, haga clic en **Asistente de clúster...** Si desea obtener más información sobre cómo configurar el Clúster de ESET con la ayuda del asistente, haga clic aquí.

Durante la configuración del Clúster de ESET hay dos formas de agregar los nodos: una automática, usando el clúster de conmutación por error o el clúster NLB actual, o examinando manualmente los ordenadores que se encuentran en un grupo de trabajo o en un dominio.

Detección automática: detecta automáticamente aquellos nodos que ya son miembros de un clúster de conmutación por error de Windows o NLB y los agrega al Clúster de ESET.
Examinar: permite agregar los nodos manualmente escribiendo el nombre de los servidores (tanto miembros del mismo grupo de trabajo como miembros del mismo dominio).

NOTA: no es necesario que los servidores sean miembros de un clúster de conmutación por error de Windows o de un clúster NLB para poder usar la función Clúster de ESET. No es necesario que haya un clúster de conmutación por error de Windows ni un clúster NLB en el entorno para poder usar los clústeres de ESET.

Tras agregar los nodos a su Clúster de ESET, el siguiente paso del proceso es instalar ESET Mail Security en cada nodo. Esta tarea se realiza automáticamente durante la configuración del Clúster de ESET.

Credenciales necesarias para la instalación remota de ESET Mail Security en otros nodos del clúster:

- Entorno de dominio: credenciales de administrador del dominio.
- Entorno de grupo de trabajo: debe asegurarse de que todos los nodos usan las credenciales de la misma cuenta de administrador local.

En un Clúster de ESET también puede usar una combinación de nodos agregados automáticamente como miembros de un clúster de conmutación por error de Windows o NLB y nodos agregados manualmente (siempre que estén en el mismo dominio).

NOTA: no es posible combinar nodos de dominio con nodos de grupo de trabajo.

Otro de los requisitos de uso del Clúster de ESET es que debe estar activada la opción **Compartir archivos e impresoras** en el Firewall de Windows antes de insertar la instalación de ESET Mail Security en los nodos de Clúster de ESET.

En caso de ser necesario, el Clúster de ESET puede desmantelarse fácilmente haciendo clic en **Destruir clúster**. Cada uno de los nodos anotará una entrada en su registro de sucesos en relación a la destrucción del Clúster de ESET. A continuación, todas las reglas del cortafuegos de ESET se eliminan del Firewall de Windows. Los antiguos nodos recuperarán su estado anterior, y pueden usarse de nuevo en otro Clúster de ESET, si así se desea.

NOTA: no es posible crear un Clúster de ESET entre ESET Mail Security y ESET File Security para Linux.

Es posible agregar nodos nuevos a un Clúster de ESET existente en cualquier momento ejecutando el **Asistente de clúster** como se ha explicado anteriormente y aquí.

5.1.10.1 Asistente de clúster: página 1

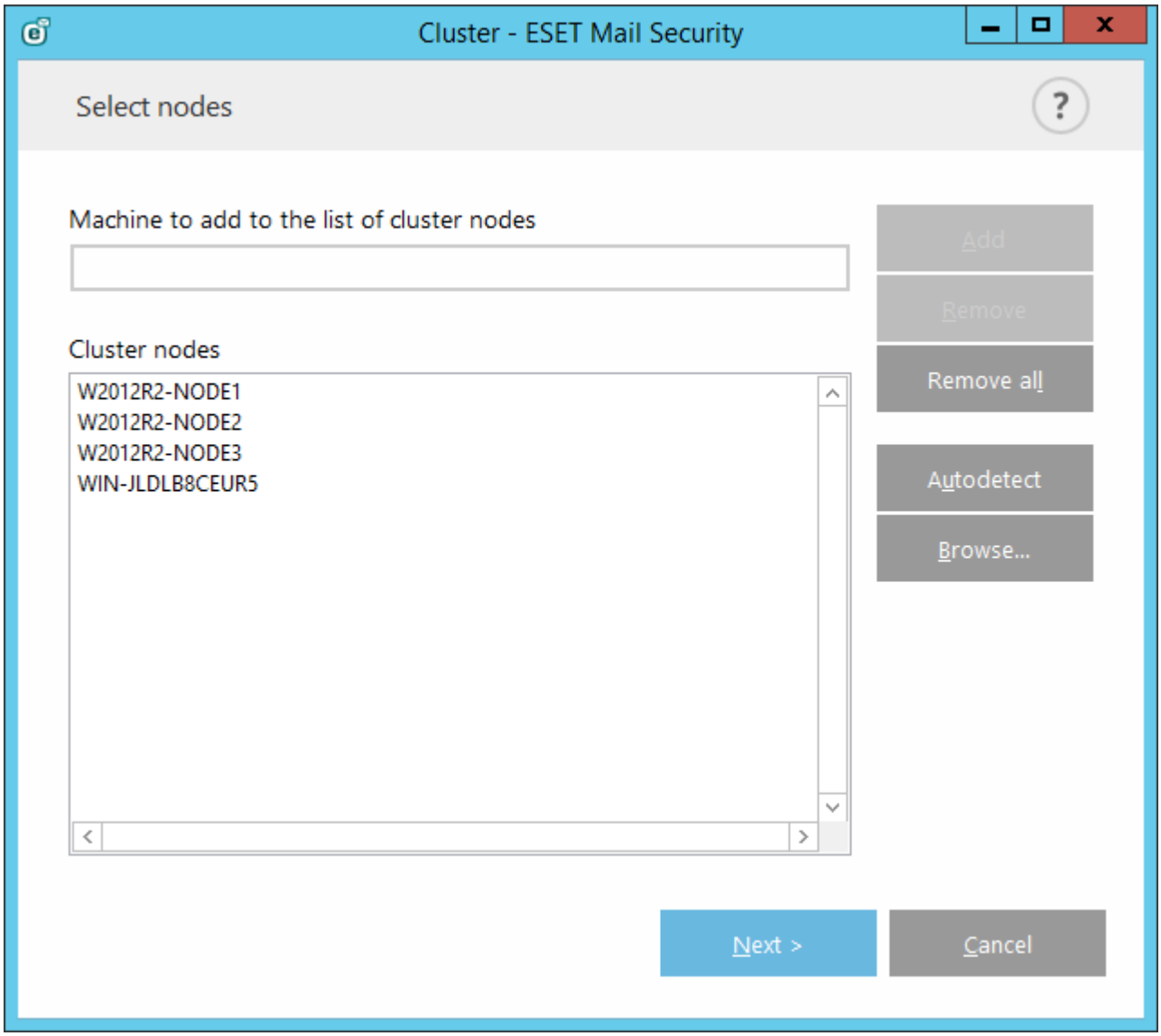
Al configurar un Clúster de ESET, el primer paso consiste en agregar los nodos. Para ello puede usar las opciones **Detección automática** o **Examinar**. También puede escribir el nombre del servidor en el cuadro de texto y hacer clic en el botón **Agregar**.

La opción **Detección automática** agrega automáticamente los nodos de un clúster de conmutación por error de Windows o de equilibrio de carga de red (NLB). Para que los nodos se agreguen automáticamente, el servidor que usa para crear el Clúster de ESET debe ser miembro de este clúster de conmutación por error de Windows o de NLB. El clúster de NLB debe tener activada la función **Permitir control remoto** en las propiedades del clúster para que el Clúster de ESET detecte los nodos correctamente. Una vez que tenga la lista de nodos recién agregados podrá quitar los nodos no deseados, en caso de que quiera que solo nodos concretos formen parte del Clúster de ESET.

Haga clic en **Examinar** para para encontrar y seleccionar ordenadores de un dominio o grupo de trabajo. Este método permite agregar manualmente los nodos al Clúster de ESET.

Otra de las formas de agregar nodos es escribir el nombre de host del servidor que desea agregar y hacer clic en **Agregar**.

Los **Nodos del clúster** actuales elegidos se agregarán al Clúster de ESET tras hacer clic en **Siguiente**:



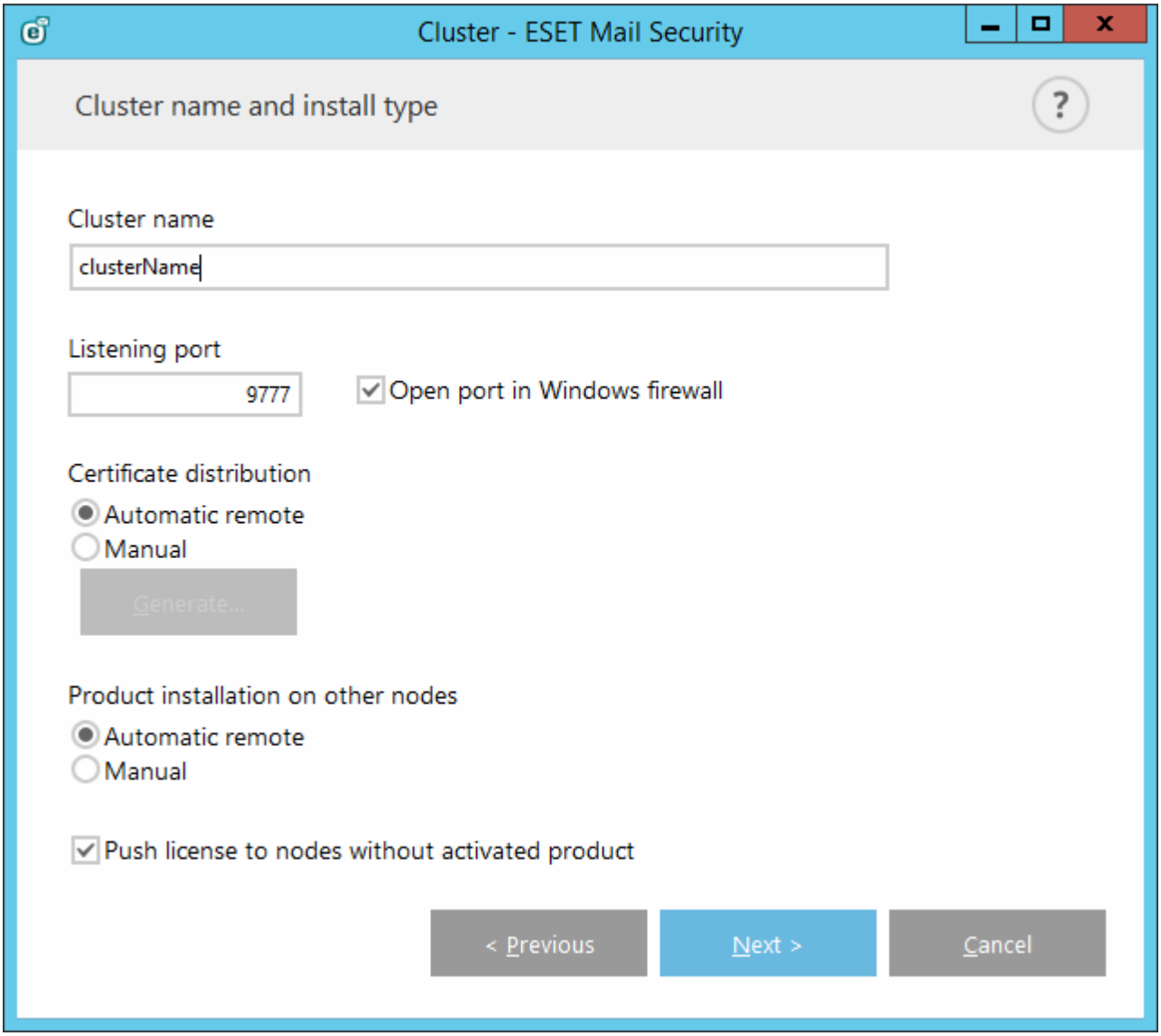
Si desea modificar los **Nodos del clúster** que aparecen en la lista, seleccione el nodo que desee quitar y haga clic en **Quitar**. Si desea borrar la lista por completo, haga clic en **Quitar todo**.

Si ya dispone de un Clúster de ESET existente, puede agregar nodos nuevos en cualquier momento. Los pasos son los mismos que los descritos anteriormente.

NOTA: todos los nodos que permanezcan en la lista deben estar en línea y ser accesibles. El host local se agrega a los nodos del clúster de forma predeterminada.

5.1.10.2 Asistente de clúster: página 2

Defina el nombre del clúster, el modo de distribución del certificado y si desea instalar el producto en los nodos o no.



Nombre del clúster: escriba el nombre del clúster.
Puerto de escucha: (el puerto predeterminado es el 9777)
Abrir puerto en el cortafuegos de Windows: cuando esta opción se activa, se crea una regla en el Firewall de Windows.

Distribución de certificado:
Remoto automático: el certificado se instalará automáticamente.
Manual: cuando hace clic en **Generar** se abre una ventana desde la que examinar; seleccione la carpeta en la que desea guardar los certificados. Se crea tanto un certificado raíz como un certificado para cada nodo, incluido el que se crea para el nodo (máquina local) desde el que está configurando el Clúster de ESET. Posteriormente podrá optar por inscribir el certificado en la máquina local haciendo clic en **Sí**. Más tarde tendrá que importar los certificados manualmente, como se describe aquí.

Instalación del producto en otros nodos:
Remoto automático: ESET Mail Security se instalará automáticamente en cada nodo (siempre que los sistemas operativos tengan la misma arquitectura).
Manual: seleccione esta opción si desea instalar ESET Mail Security manualmente (por ejemplo, cuando tiene arquitecturas de SO distintas en algunos nodos).

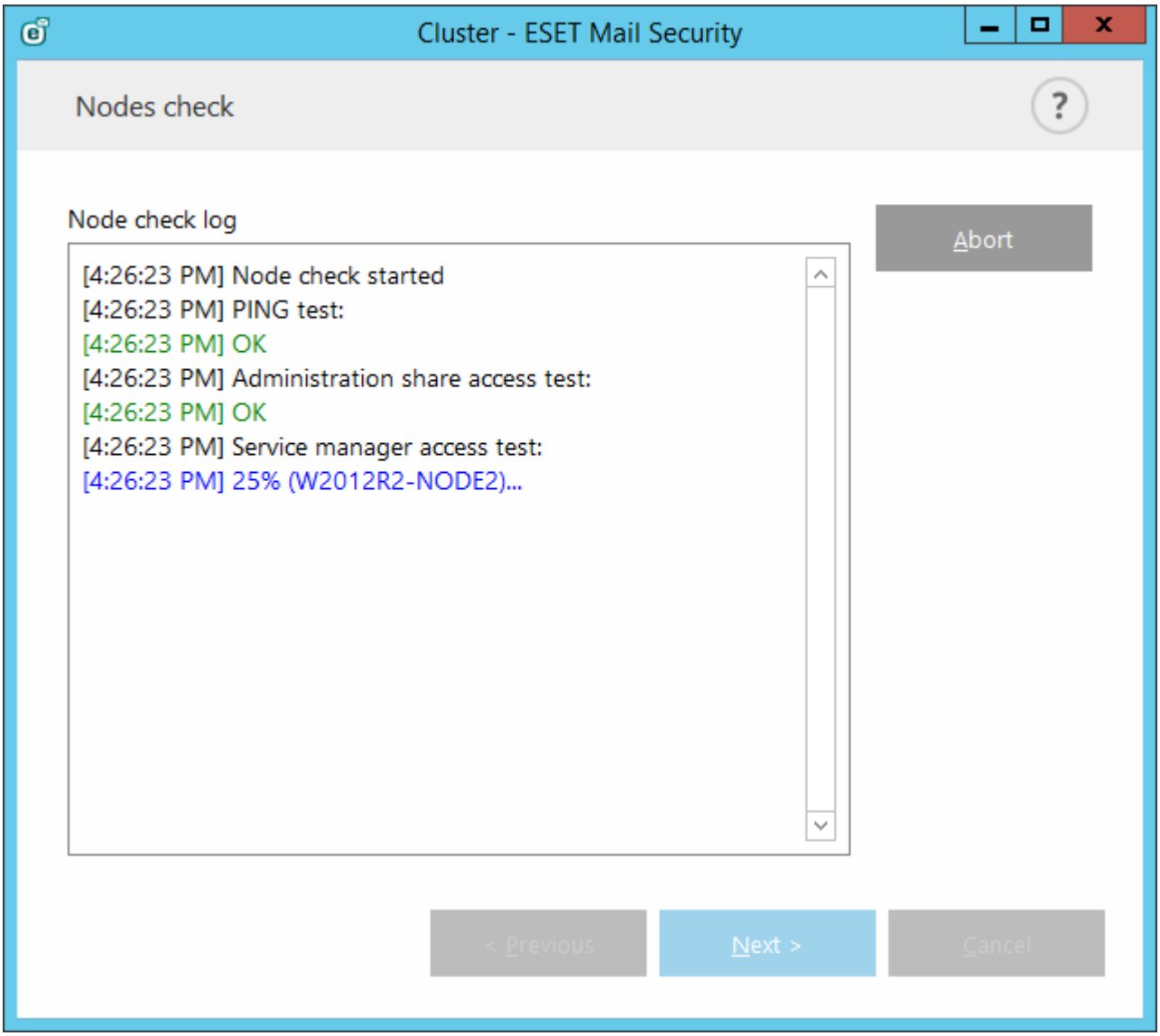
Enviar licencia a nodos sin el producto activado: cuando esta opción esté activada, los nodos recibirán ESET Mail Security activado.

NOTA: si desea crear un Clúster de ESET con arquitecturas de sistema operativo mixtas (32 bits y 64 bits), tendrá que instalar ESET Mail Security manualmente. Esto se detectará durante los próximos pasos, y verá esta información en la ventana de registro.

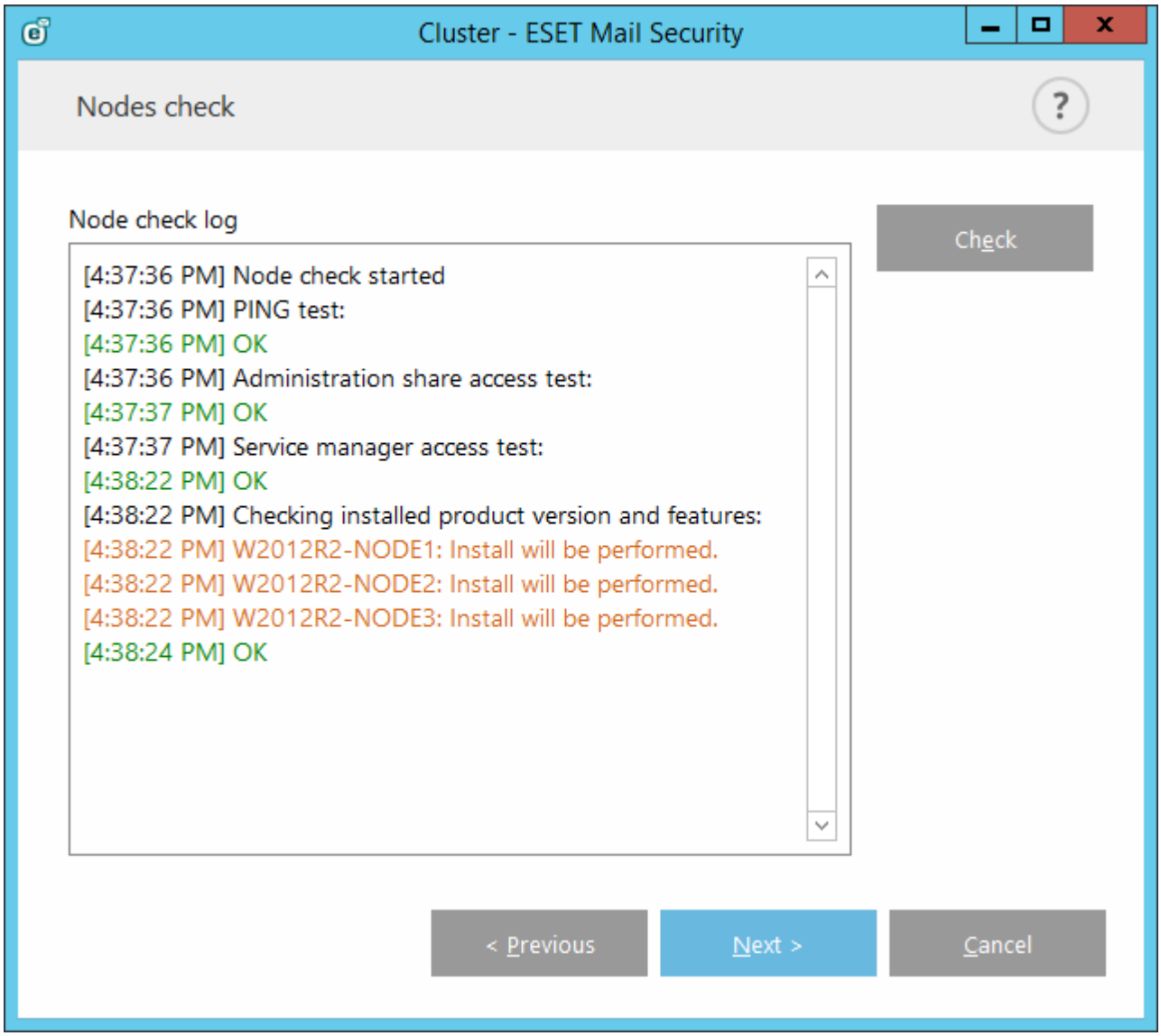
5.1.10.3 Asistente de clúster: página 3

Después de especificarse los detalles de la instalación se ejecuta una comprobación de nodos. En el **Registro de comprobación de nodos** podrá consultar las siguientes comprobaciones:

- Comprobación de que todos los nodos existentes están en línea.
- Comprobación de que puede accederse a los nodos nuevos.
- El nodo está en línea.
- Puede accederse al recurso compartido de administración.
- Es posible la ejecución remota.
- Está instalada la versión correcta del producto, o no hay producto (solo si se seleccionó la instalación automática).
- Comprobación de que están presentes los nuevos certificados.

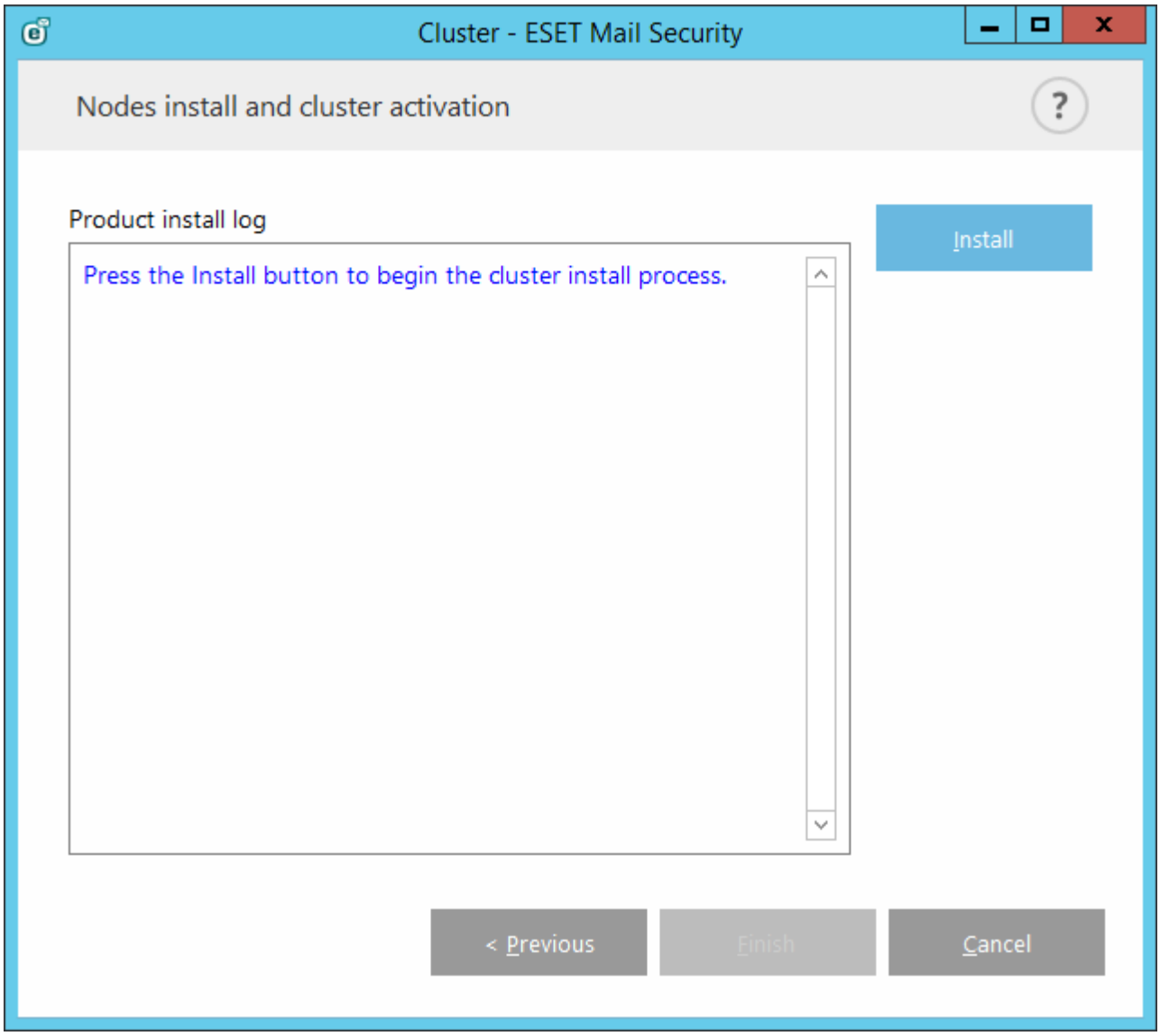


Verá el informe cuando concluya la comprobación de nodos:


Cluster - ESET Mail Security
Nodes check
Node check log
Check
[4:37:36 PM] Node check started
[4:37:36 PM] PING test:
[4:37:36 PM] OK
[4:37:36 PM] Administration share access test:
[4:37:37 PM] OK
[4:37:37 PM] Service manager access test:
[4:38:22 PM] OK
[4:38:22 PM] Checking installed product version and features:
[4:38:22 PM] W2012R2-NODE1: Install will be performed.
[4:38:22 PM] W2012R2-NODE2: Install will be performed.
[4:38:22 PM] W2012R2-NODE3: Install will be performed.
[4:38:24 PM] OK
< Previous
Next >
Cancel

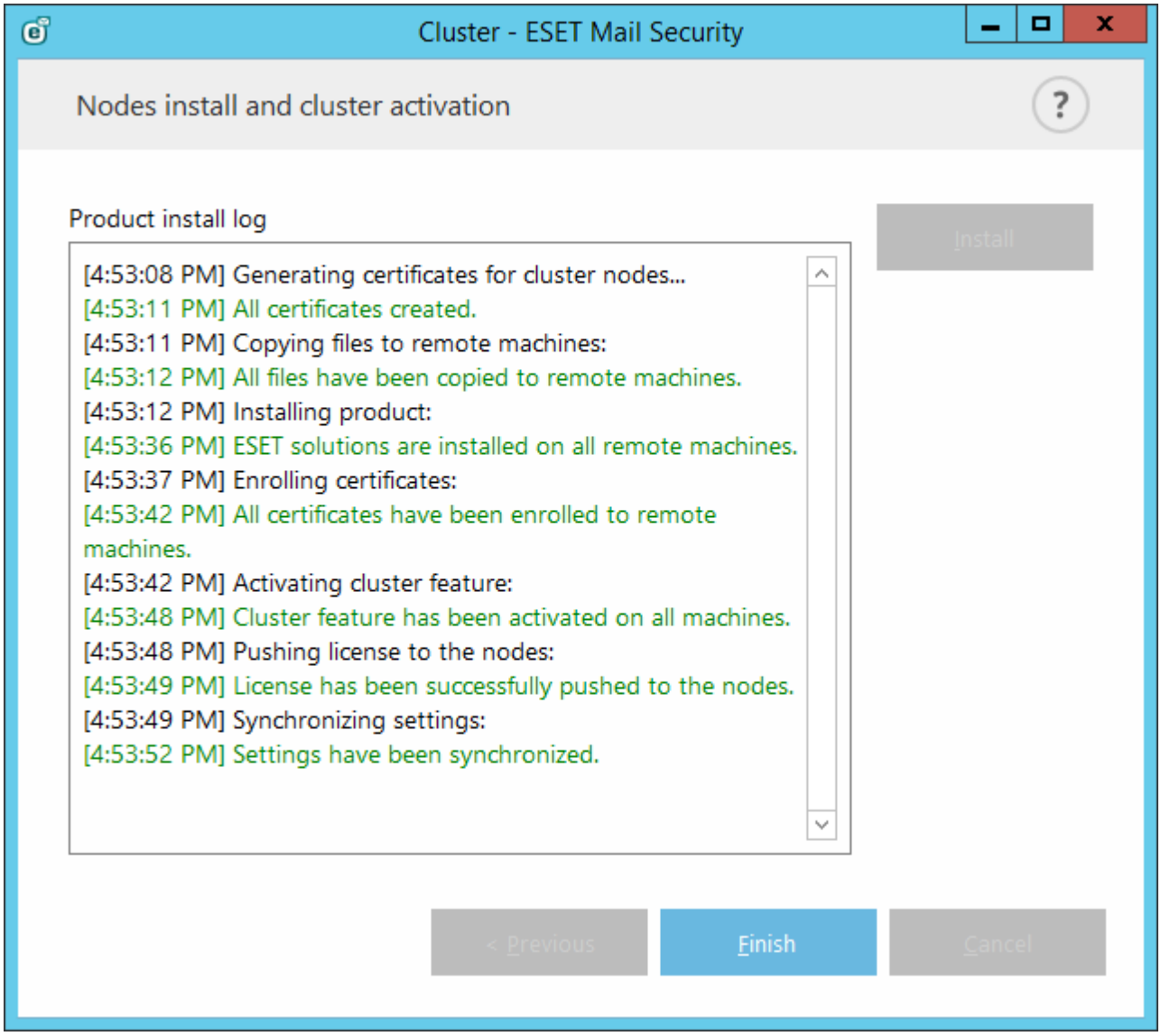
5.1.10.4 Asistente de clúster: página 4

Cuando el producto debe instalarse en una máquina remota durante la inicialización del Clúster de ESET, el paquete de instalación se busca en el directorio %ProgramData%\ESET\<Nombre_producto>\Installer. Si no se encuentra el paquete de instalación en este directorio, se pide al usuario que indique su ubicación.

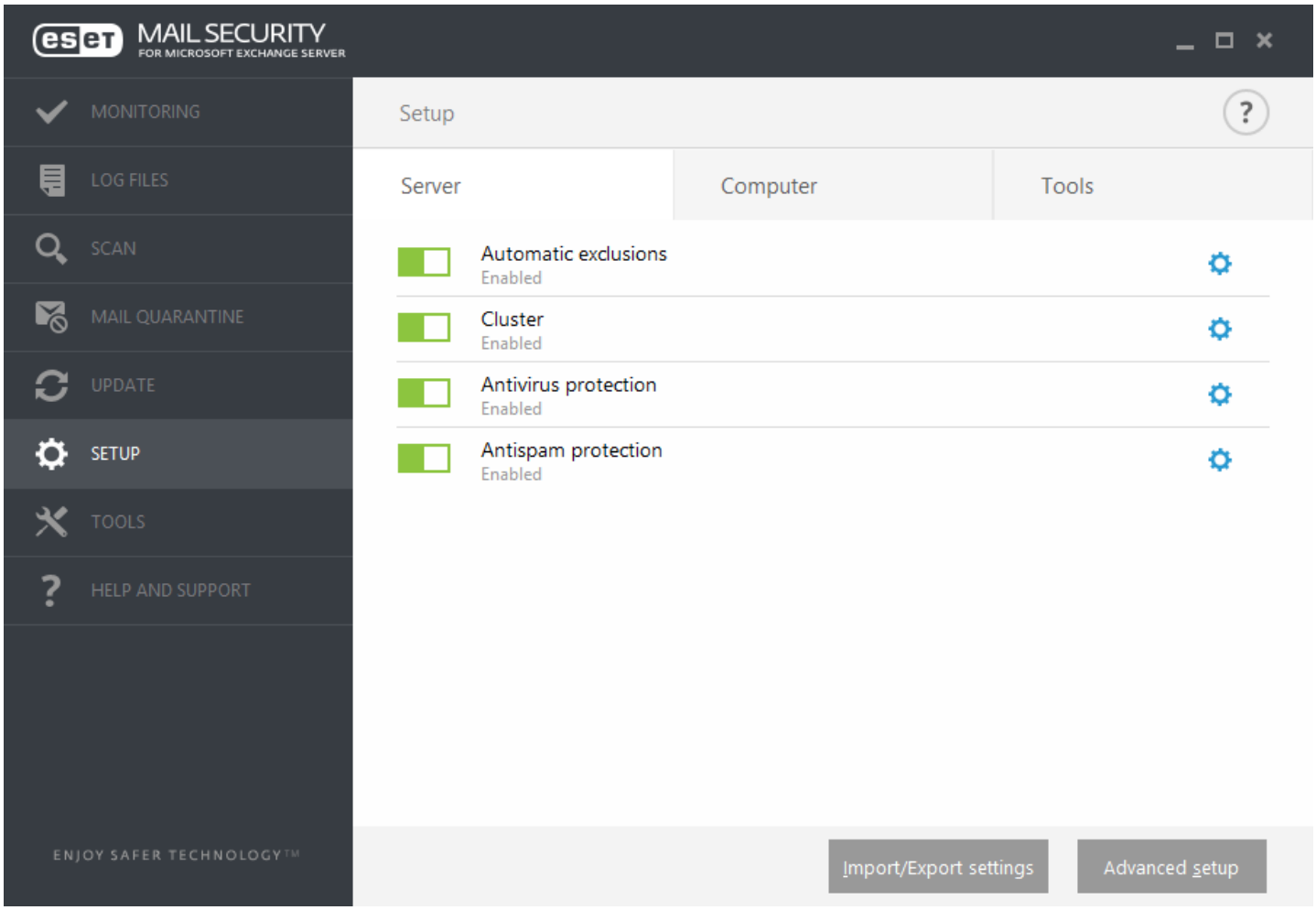


NOTA: al intentar usar la instalación remota automática en un nodo con una plataforma distinta (32 bits frente a 64 bits) se detectará esta situación y se recomendará la instalación manual para este nodo.

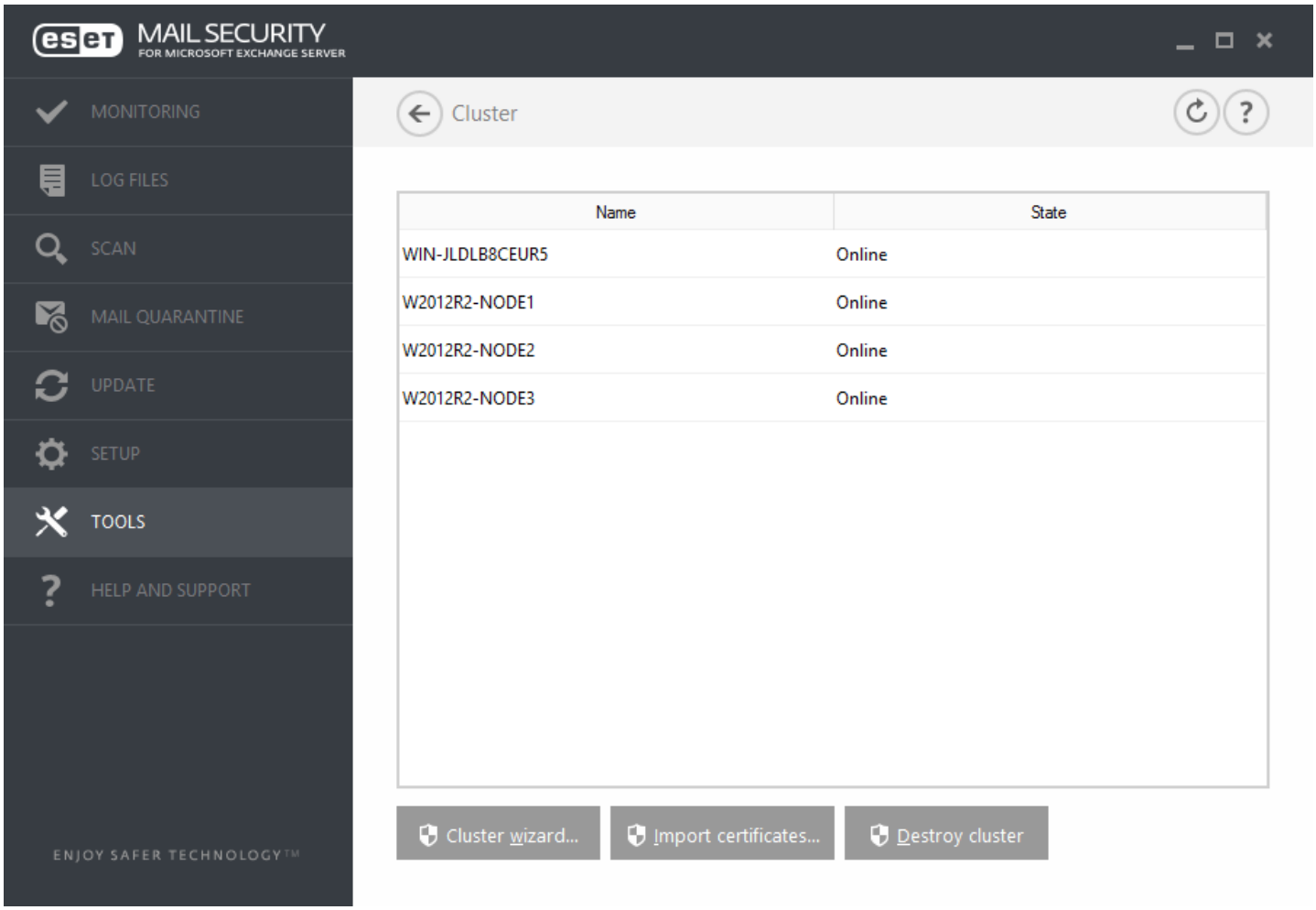
NOTA: si tiene una versión de ESET Mail Security más antigua instalada en algunos nodos, ESET Mail Security debe reinstalarse con una versión más reciente en estas máquinas antes de crearse el clúster. Esto podría provocar un reinicio automático de estas máquinas. En caso de darse esta situación, se mostrará una advertencia.


Cluster - ESET Mail Security
Nodes install and cluster activation
Product install log
Install
[4:53:08 PM] Generating certificates for cluster nodes...
[4:53:11 PM] All certificates created.
[4:53:11 PM] Copying files to remote machines:
[4:53:12 PM] All files have been copied to remote machines.
[4:53:12 PM] Installing product:
[4:53:36 PM] ESET solutions are installed on all remote machines.
[4:53:37 PM] Enrolling certificates:
[4:53:42 PM] All certificates have been enrolled to remote machines.
[4:53:42 PM] Activating cluster feature:
[4:53:48 PM] Cluster feature has been activated on all machines.
[4:53:48 PM] Pushing license to the nodes:
[4:53:49 PM] License has been successfully pushed to the nodes.
[4:53:49 PM] Synchronizing settings:
[4:53:52 PM] Settings have been synchronized.
< Previous
Finish
Cancel

Una vez que haya configurado correctamente el Clúster de ESET, este aparecerá en la página **Configuración** > **Servidor** como activado.



Además, puede consultar su estado actual en la página de estado del clúster (**Herramientas** > **Clúster**).



Importar certificados...

- Desplácese hasta la carpeta que contiene los certificados (generada con el Asistente de clúster). Seleccione el archivo de certificado y haga clic en **Abrir**.

5.2 Ordenador

El módulo **Ordenador** está disponible en **Configuración** > **Ordenador**. En él se muestra una visión general de los módulos de protección que se describen en el capítulo anterior. En esta sección están disponibles los parámetros siguientes:

- Protección del sistema de archivos en tiempo real
- Análisis del ordenador a petición
- Análisis de estado inactivo
- Análisis en el inicio
- Medios extraíbles
- Protección de documentos
- HIPS

Las **Opciones de análisis** de todos los módulos de protección (por ejemplo, protección del sistema de archivos en tiempo real, protección del tráfico de Internet, etc.) le permiten activar o desactivar la detección de los siguientes elementos:

- Las aplicaciones potencialmente indeseables (PUA) no tienen por qué ser maliciosas, pero pueden afectar al rendimiento del ordenador de forma negativa.
  Puede obtener más información sobre estos tipos de aplicaciones en el glosario.
- Por aplicaciones potencialmente peligrosas se entienden programas de software comercial legítimo que pueden utilizarse con fines maliciosos. Entre los ejemplos de este tipo de programas encontramos herramientas de acceso

remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que registran cada tecla pulsada por un usuario). Esta opción está desactivada de manera predeterminada.
Puede obtener más información sobre estos tipos de aplicaciones en el glosario.

- Entre las **Aplicaciones potencialmente peligrosas** se incluyen programas comprimidos con empaquetadores o protectores. Los autores de código malicioso con frecuencia explotan estos tipos de protectores para evitar ser detectados.

La **Tecnología Anti-Stealth** es un sofisticado sistema de detección de programas peligrosos (como los rootkits), que pueden ocultarse del sistema operativo, lo que hace que no sea posible detectarlos mediante las técnicas habituales.

Exclusiones de procesos le permite excluir procesos concretos. Por ejemplo, en el caso de los procesos de la solución de copia de seguridad, donde todas las operaciones con archivos relacionadas con dichos procesos excluidos se ignoran y se consideran seguras, minimizando de este modo las interferencias con el proceso de copia de seguridad.

Las exclusiones le permiten excluir archivos y carpetas del análisis. Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. Puede que haya situaciones en las que necesite excluir un objeto, como durante el análisis de entradas de una base de datos grande que ralentice el ordenador o software que entre en conflicto con el análisis. Para obtener instrucciones sobre cómo excluir un objeto del análisis, consulte Exclusiones.

5.2.1 Detección de una amenaza

Las amenazas pueden acceder al sistema desde varios puntos de entrada, como páginas web, carpetas compartidas, correo electrónico o dispositivos extraíbles (USB, discos externos, CD, DVD, disquetes, etc.).

Comportamiento estándar

Como ejemplo general de la forma en la que ESET Mail Security gestiona las amenazas, estas se pueden detectar mediante:

- Protección del sistema de archivos en tiempo real
- Protección del tráfico de Internet
- Protección del cliente de correo electrónico
- Análisis del ordenador

Cada uno de estos componentes utiliza el nivel de desinfección estándar e intentará desinfectar el archivo y moverlo a Cuarentena o finalizar la conexión. Se muestra una ventana de notificación en el área de notificación, situada en la esquina inferior derecha de la pantalla. Para obtener más información sobre los tipos de desinfección y el comportamiento, consulte la sección Desinfección.

Desinfección y eliminación

Si no hay que realizar ninguna acción predefinida para la protección en tiempo real, se le pedirá que seleccione una opción en la ventana de alerta. Normalmente, están disponibles las opciones **Desinfectar**, **Eliminar** y **Sin acciones**. No se recomienda seleccionar **Sin acciones**, ya que los archivos infectados quedarían intactos. La única excepción es cuando está seguro de que el archivo es inofensivo y se ha detectado por error.

Aplique esta opción si un archivo ha sido infectado por un virus que le ha añadido código malicioso. Si este es el caso, primero intente desinfectar el archivo infectado para restaurarlo a su estado original. Si el archivo consta exclusivamente de código malicioso, se eliminará.

Si un proceso del sistema "bloquea" o está utilizando un archivo infectado, por lo general solo se eliminará cuando se haya publicado (normalmente, tras reiniciar el sistema).

Múltiples amenazas

Si durante un análisis del ordenador no se desinfectaron algunos archivos infectados (o el Nivel de desinfección se estableció en **Sin desinfección**), aparecerá una ventana de alerta solicitándole que seleccione las acciones que desea llevar a cabo en esos archivos. Seleccione una acción individualmente para cada una de las amenazas de la

lista, o utilice **Seleccionar acción para todas las amenazas de la lista**, elija la acción que desea realizar en todas las amenazas de la lista y, a continuación, haga clic en **Finalizar**.

Eliminación de amenazas de archivos comprimidos

En el modo de desinfección predeterminado, solo se eliminará todo el archivo comprimido si todos los archivos que contiene están infectados. En otras palabras, los archivos comprimidos no se eliminan si también contienen archivos no infectados e inofensivos. Tenga cuidado cuando realice un análisis con desinfección exhaustiva activada, ya que un archivo comprimido se eliminará si contiene al menos un archivo infectado, sin tener en cuenta el estado de los otros archivos.
Si el ordenador muestra señales de infección por código malicioso —por ejemplo, se ralentiza, se bloquea con frecuencia, etc.—, le recomendamos que haga lo siguiente:

- Abra ESET Mail Security y haga clic en Análisis del ordenador.
- Haga clic en **Análisis estándar** (para obtener más información, consulte Análisis del ordenador).
- Una vez que haya finalizado el análisis, revise el registro para consultar el número de archivos analizados, infectados y desinfectados.

Si solo desea analizar una parte específica del disco, haga clic en **Análisis personalizado** y seleccione los objetos que desea incluir en el análisis de virus.

5.2.2 Exclusiones de procesos

Esta función le permite excluir procesos de aplicaciones del análisis de acceso del antivirus. Estas exclusiones ayudan a minimizar el riesgo de posibles conflictos y a mejorar el rendimiento de las aplicaciones excluidas, lo que a su vez tiene una repercusión positiva en el rendimiento global del sistema operativo.

Cuando un proceso se excluye, su archivo ejecutable no se supervisa. La actividad del proceso excluido no se supervisa mediante ESET Mail Security, y no se realiza análisis alguno de las operaciones de archivos efectuadas por el proceso.

Utilice **Agregar**, **Modificar** y **Quitar** para gestionar la exclusión de procesos.

NOTA: las exclusiones de procesos suponen exclusiones únicamente del análisis de acceso del antivirus. Por ejemplo, la protección del acceso a la Web no tiene en cuenta esta exclusión, por lo que si excluye el archivo ejecutable de su navegador web, los archivos descargados se seguirán analizando. De esta forma pueden detectarse las amenazas. Esta situación tiene meramente fines ilustrativos, y no se recomienda crear exclusiones para los navegadores web.

NOTA: el HIPS se encarga de la evaluación de los procesos excluidos, por lo que se recomienda que pruebe los nuevos procesos excluidos con el HIPS activado (o desactivado si le surgen problemas). La desactivación del HIPS no afectará a las exclusiones de procesos. Si el HIPS está desactivado, la identificación de los procesos excluidos se basa únicamente en la ruta.

5.2.3 Exclusiones automáticas

Los desarrolladores de aplicaciones de servidor y sistemas operativos recomiendan, en la mayoría de sus productos, excluir conjuntos de archivos y carpetas de trabajo críticos de los análisis antivirus. Los análisis antivirus pueden tener un efecto negativo sobre el rendimiento del servidor, provocar conflictos e incluso evitar la ejecución de determinadas aplicaciones en el servidor. Las exclusiones minimizan el riesgo de sufrir conflictos y aumentan el rendimiento general del servidor durante la ejecución de software antivirus.

ESET Mail Security identifica las aplicaciones de servidor y los archivos del sistema operativo críticas, y los añade a la lista de exclusiones. Puede ver una lista de las aplicaciones de servidor detectadas, para las que se crearon exclusiones, en **Exclusiones automáticas que generar**. De forma predeterminada están activadas todas las exclusiones automáticas. Puede desactivar/activar cada aplicación de servidor al hacer clic en el conmutador con el siguiente resultado:

1. Si la exclusión de una aplicación o un sistema operativo sigue activada, sus archivos y carpetas críticos se añadirán a la lista de archivos excluidos del análisis (**Configuración avanzada** > **Ordenador** > **Básico** > **Exclusiones** > **Editar**). Cada vez que se reinicia el servidor, el sistema realiza una comprobación automática de las exclusiones y restaura las exclusiones que se hayan podido eliminar de la lista. Esta es la configuración recomendada para garantizar que se aplican siempre las exclusiones automáticas recomendadas.

2. Si el usuario desactiva la exclusión de una aplicación o un sistema operativo, sus archivos y carpetas críticos permanecerán en la lista de archivos excluidos del análisis (**Configuración avanzada** > **Ordenador** > **Básico** > **Exclusiones** > **Editar**). Sin embargo, no se comprobarán ni renovarán automáticamente en la lista **Exclusiones** cada vez que se reinicie el servidor (consulte el punto 1 anterior). Esta configuración se recomienda a los usuarios avanzados que deseen eliminar o modificar algunas de las exclusiones estándar. Si desea que las exclusiones se eliminen de la lista sin reiniciar el servidor, quítelas manualmente (**Configuración avanzada** > **Ordenador** > **Básico** > **Exclusiones** > **Editar**).

Las exclusiones definidas por el usuario introducidas manualmente (en **Configuración avanzada** > **Ordenador** > **Básico** > **Exclusiones** > **Editar**) no se verán afectadas por los ajustes descritos anteriormente.

Las exclusiones automáticas de aplicaciones de servidor o sistemas operativos se seleccionan de acuerdo con las recomendaciones de Microsoft. Si desea obtener más información, consulte los siguientes artículos de la Knowledge Base de Microsoft:

- Recomendaciones para la detección de virus en equipos de empresa que ejecutan actualmente versiones compatibles de Windows
- Recomendaciones para solucionar problemas de un equipo con Exchange Server con software antivirus instalado
- Recomendaciones para el uso de análisis de nivel de archivo con Exchange 2007
- Software antivirus en el sistema operativo de servidores Exchange

5.2.4 Caché local compartida

La caché local compartida mejora el rendimiento en entornos virtualizados al eliminar el análisis duplicado en la red. De esta manera se garantiza que cada archivo se analizará solo una vez y se almacenará en la caché compartida. Active el conmutador **Activar caché** para guardar en la caché local información sobre los análisis de archivos y carpetas de su red. Si realiza un análisis nuevo, ESET Mail Security buscará los archivos analizados en la caché. Si los archivos coinciden, no se incluirán en el análisis.

La configuración de **Servidor de caché** contiene los campos siguientes**:**

- **Nombre de host**: nombre o dirección IP del ordenador donde se encuentra la caché.
- **Puerto**: número de puerto utilizado para la comunicación (el mismo que se estableció en la caché local compartida).
- **Contraseña**: especifique la contraseña de la caché local compartida, si es necesario.

5.2.5 Rendimiento

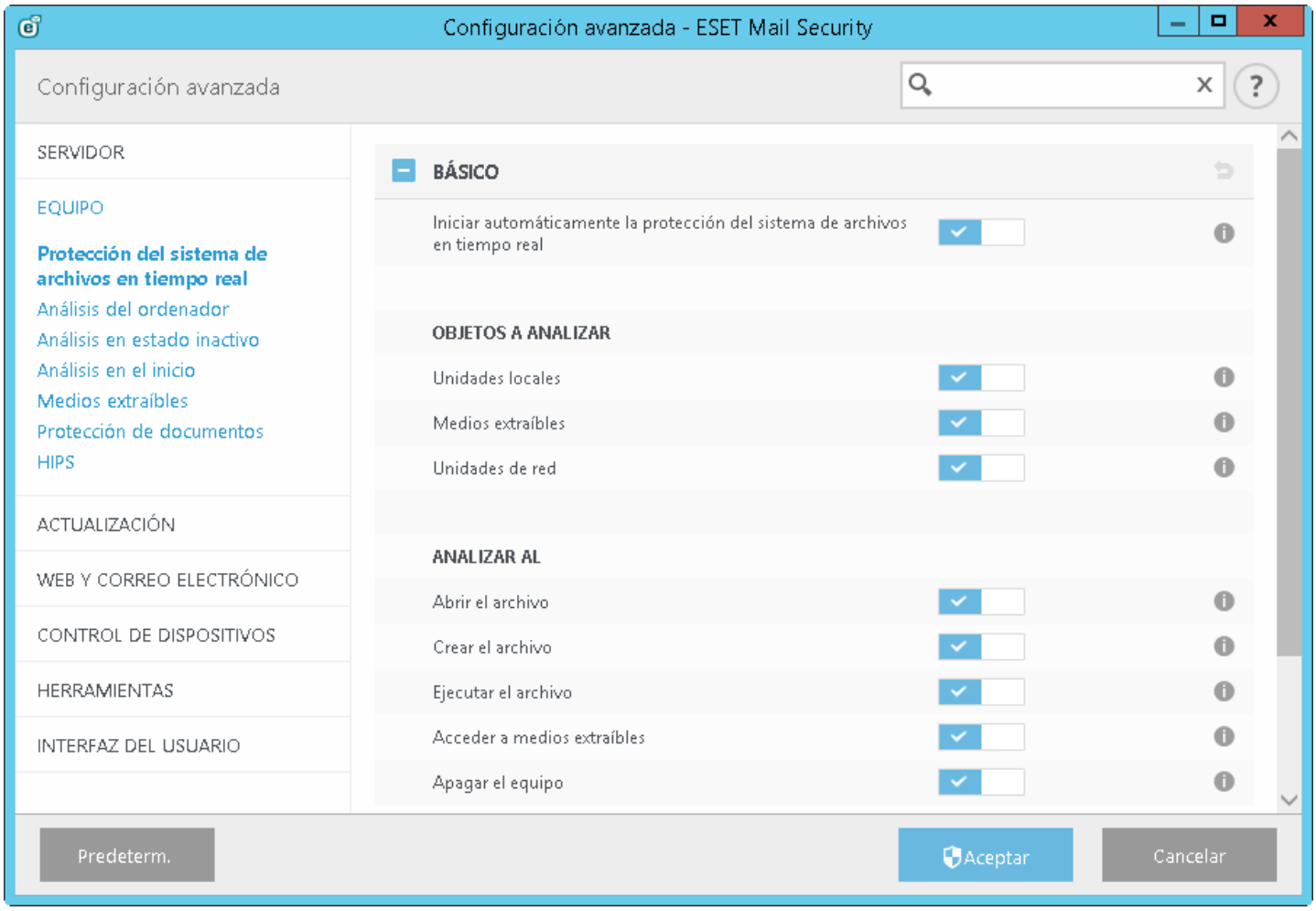
Es posible establecer el número de motores de análisis ThreatSense independientes utilizados por la protección antivirus y antiespía al mismo tiempo.

Si no existe ningún tipo de restricciones, se recomienda aumentar el número de motores de análisis de ThreatSense según la siguiente fórmula: *número de motores de análisis de ThreatSense = (número de CPU físicas x 2) + 1*.

NOTA: El valor aceptable oscila entre 1 y 20, lo que significa que el número máximo de motores de análisis de ThreatSense que puede usar es 20.

5.2.6 Protección del sistema de archivos en tiempo real

La protección del sistema de archivos en tiempo real controla todos los sucesos relacionados con el antivirus en el sistema. Todos los archivos se analizan en busca de código malicioso en el momento de abrirlos, crearlos o ejecutarlos en el ordenador. La protección del sistema de archivos en tiempo real se inicia al arrancar el sistema.



La protección del sistema de archivos en tiempo real comienza de forma predeterminada cuando se inicia el sistema y proporciona un análisis ininterrumpido. En caso especiales (por ejemplo, si hay un conflicto con otro análisis en tiempo real), puede desactivar la protección en tiempo real anulando la selección de **Iniciar automáticamente la protección del sistema de archivos en tiempo real**, en la sección **Protección del sistema de archivos en tiempo real** > **Básico** de Configuración avanzada.

- **Objetos a analizar**

De forma predeterminada, se buscan posibles amenazas en todos los tipos de objetos:

Unidades locales: controla todas las unidades de disco duro del sistema.
Medios extraíbles: controla los discos CD y DVD, el almacenamiento USB, los dispositivos Bluetooth, etc.
Unidades de red: analiza todas las unidades asignadas.

Recomendamos que esta configuración predeterminada se modifique solo en casos específicos como, por ejemplo, cuando el control de ciertos objetos ralentiza significativamente las transferencias de datos.

- **Analizar**

De forma predeterminada, todos los archivos se analizan cuando se abren, crean o ejecutan. Le recomendamos que mantenga esta configuración predeterminada, ya que ofrece el máximo nivel de protección en tiempo real para su ordenador:

- **Abrir el archivo**: activa o desactiva el análisis al abrir archivos.
- **Crear el archivo**: activa o desactiva el análisis durante la creación de archivos.
- **Ejecutar el archivo**: activa o desactiva el análisis cuando se ejecutan archivos.
- **Acceso a medios extraíbles**: activa o desactiva el análisis activado por el acceso a determinados medios extraíbles con espacio de almacenamiento.
- **Apagar el equipo**: activa o desactiva el análisis activado por el apagado del ordenador.

La protección del sistema de archivos en tiempo real comprueba todos los tipos de medios y se activa con varios sucesos del sistema como, por ejemplo, cuando se accede a un archivo. Si se utilizan métodos de detección con la tecnología ThreatSense (tal como se describe en la sección Parámetros de ThreatSense), la protección del sistema de archivos en tiempo real se puede configurar para que trate de forma diferente los archivos recién creados y los archivos existentes. Por ejemplo, puede configurar la protección del sistema de archivos en tiempo real para que supervise más detenidamente los archivos recién creados.

Con el fin de que el impacto en el sistema sea mínimo cuando se utiliza la protección en tiempo real, los archivos que ya se analizaron no se vuelven a analizar (a no ser que se hayan modificado). Los archivos se vuelven a analizar inmediatamente después de cada actualización de la base de firmas de virus. Este comportamiento se controla con la opción **Optimización inteligente**. Si la opción Optimización inteligente está desactivada, se analizan todos los archivos cada vez que se accede a ellos. Para modificar este ajuste, pulse **F5** para abrir Configuración avanzada y despliegue **Ordenador** > **Protección del sistema de archivos en tiempo real**. Haga clic en **Parámetros de ThreatSense** > **Otros** y seleccione o anule la selección de **Activar optimización inteligente**.

5.2.6.1 Exclusiones

No debe confundirse con **Extensiones excluidas**

Las exclusiones le permiten excluir archivos y carpetas del análisis. Para garantizar que se analizan todos los objetos en busca de amenazas, le recomendamos que solo cree exclusiones cuando sea absolutamente necesario. Puede que haya situaciones en las que necesite excluir un objeto, como durante el análisis de entradas de una base de datos grande que ralentice el ordenador o software que entre en conflicto con el análisis (por ejemplo, software de copia de seguridad).

Para excluir un objeto del análisis:

Haga clic en **Agregar** y especifique la ruta de acceso de un objeto o selecciónela en la estructura de árbol.
Puede utilizar comodines para abarcar un grupo de archivos. El signo de interrogación (?) representa un carácter único variable y el asterisco (*), una cadena variable de cero o más caracteres.

Ejemplos

- Si desea excluir todos los archivos de una carpeta, escriba la ruta a la carpeta y utilice la máscara "*.*".
- Para excluir una unidad entera incluidos archivos y subcarpetas, utilice la máscara "D:*".
- Si desea excluir únicamente los archivos .doc, utilice la máscara "*.doc".
- Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (y los caracteres varían) y solo conoce con seguridad el primero (por ejemplo, "D"), utilice el siguiente formato: "D????.exe". Los símbolos de interrogación sustituyen a los caracteres que faltan (desconocidos).

NOTA: el módulo de protección del sistema de archivos en tiempo real o de análisis del ordenador no detectará las amenazas que contenga un archivo si este cumple los criterios de exclusión del análisis.

Columnas

Ruta: ruta de los archivos y carpetas excluidos.
Amenaza: si se muestra el nombre de una amenaza junto a un archivo excluido, significa que el archivo se excluye únicamente para dicha amenaza. Si este archivo se infecta más adelante con otro código malicioso, el módulo antivirus lo detectará. Este tipo de exclusión únicamente se puede utilizar para determinados tipos de amenazas, y se puede crear bien en la ventana de alerta de amenaza que informa de la amenaza (haga clic en **Más información** y, a continuación, seleccione **Excluir de la detección**) o bien en **Herramientas** > **Cuarentena**, haciendo clic con el botón derecho del ratón en el archivo en cuarentena y seleccionando **Restaurar y excluir del análisis** en el menú contextual.

Elementos de control

Agregar: excluye los objetos de la detección.
Editar: le permite modificar las entradas seleccionadas.
Quitar: elimina las entradas seleccionadas.

5.2.6.1.1 Agregar o modificar exclusiones

Este cuadro de diálogo le permite agregar o modificar exclusiones. Se puede realizar de dos maneras:

- Escribiendo la ruta de un objeto que se desea excluir.
- Seleccionándola en la estructura de árbol (haga clic en los **...** que aparecen al final del campo de texto para examinar).

El primer método permite utilizar los comodines descritos en la sección Formato de exclusión.

5.2.6.1.2 Formato de exclusión

Puede utilizar comodines para abarcar un grupo de archivos. El signo de interrogación (?) representa un carácter único variable y el asterisco (*), una cadena variable de cero o más caracteres.

Ejemplos

- Si desea excluir todos los archivos de una carpeta, escriba la ruta a la carpeta y utilice la máscara "*.*".
- Para excluir una unidad entera incluidos archivos y subcarpetas, utilice la máscara "D:*".
- Si desea excluir únicamente los archivos .doc, utilice la máscara "*.doc".
- Si el nombre de un archivo ejecutable tiene un determinado número de caracteres (y los caracteres varían) y solo conoce con seguridad el primero (por ejemplo, "D"), utilice el siguiente formato: "D????.exe". Los símbolos de interrogación sustituyen a los caracteres que faltan (desconocidos).

5.2.6.2 Parámetros de ThreatSense

La tecnología ThreatSense consta de muchos métodos complejos de detección de amenazas. Esta tecnología es proactiva, lo que significa que también proporciona protección durante la fase inicial de expansión de una nueva amenaza. Utiliza una combinación de análisis de código, emulación de código, firmas genéricas y firmas de virus que funcionan de forma conjunta para mejorar en gran medida la seguridad del sistema. El motor de análisis es capaz de controlar varios flujos de datos de forma simultánea, de manera que maximiza la eficacia y la velocidad de detección. Además, la tecnología ThreatSense elimina los rootkits eficazmente.

NOTA: para obtener más información sobre la comprobación automática de los archivos en el inicio, consulte Análisis en el inicio.

Las opciones de configuración del motor ThreatSense permiten al usuario especificar distintos parámetros de análisis:

- Los tipos de archivos y extensiones que se deben analizar.
- La combinación de diferentes métodos de detección.
- Los niveles de desinfección, etc.

Para acceder a la ventana de configuración, haga clic en **Configuración de los parámetros del motor ThreatSense** en la ventana Configuración avanzada de cualquier módulo que utilice la tecnología ThreatSense (consulte a continuación). Es posible que cada contexto de seguridad requiera una configuración diferente. Con esto en mente, ThreatSense se puede configurar individualmente para los siguientes módulos de protección:

- Protección del sistema de archivos en tiempo real
- Análisis de estado inactivo
- Análisis en el inicio
- Protección de documentos
- Protección del cliente de correo electrónico
- Protección del tráfico de Internet
- Análisis del ordenador

Los parámetros de ThreatSense están altamente optimizados para cada módulo y su modificación puede afectar al funcionamiento del sistema de forma significativa. Por ejemplo, la modificación de los parámetros para que siempre analicen empaquetadores de ejecución en tiempo real o la activación de la heurística avanzada en el módulo de protección del sistema de archivos en tiempo real podrían implicar la ralentización del sistema (normalmente, solo se analizan archivos recién creados mediante estos métodos). Se recomienda que no modifique los parámetros predeterminados de ThreatSense para ninguno de los módulos, a excepción de Análisis del ordenador.

Objetos a analizar

En esta sección se pueden definir los componentes y archivos del ordenador que se analizarán en busca de amenazas.

- **Memoria operativa**: busca amenazas que ataquen a la memoria operativa del sistema.
- **Sectores de inicio**: analiza los sectores de inicio para detectar virus en el registro de inicio principal (MBR). Si se trata de una máquina virtual Hyper-V, el MBR del disco se analiza en el modo de solo lectura.
- **Archivos de correo**: el programa admite las extensiones DBX (Outlook Express) y EML.
- **Archivos comprimidos**: el programa admite las extensiones ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE y muchas más.
- **Archivos comprimidos de autoextracción**: los archivos comprimidos de auto extracción (SFX) son archivos que no necesitan programas especializados (archivos) para descomprimirse.
- **Empaquetadores en tiempo real**: después de su ejecución, los empaquetadores en tiempo real (a diferencia de los archivos estándar) se descomprimen en la memoria. Además de los empaquetadores estáticos estándar (UPX, yoda, ASPack, FSG, etc.), el módulo de análisis es capaz de reconocer varios tipos de empaquetadores adicionales gracias a la emulación de códigos.

Opciones de análisis

Seleccione los métodos empleados al analizar el sistema en busca de infiltraciones. Están disponibles las opciones siguientes:

- **Heurística**: la heurística es un algoritmo que analiza la actividad (maliciosa) de los programas. La principal ventaja de esta tecnología es la habilidad para identificar software malicioso que no existía o que la base de firmas de virus anterior no conocía. Su desventaja es la probabilidad (muy pequeña) de falsas alarmas.
- **Heurística avanzada/DNA/Firmas inteligentes**: la heurística avanzada es un algoritmo heurístico único desarrollado por ESET, optimizado para detectar gusanos informáticos y troyanos escritos en lenguajes de programación de alto nivel. El uso de la heurística avanzada mejora en gran medida la detección de amenazas por parte de los productos de ESET. Las firmas pueden detectar e identificar virus de manera fiable. Gracias al sistema de actualización automática, las nuevas firmas están disponibles en cuestión de horas cuando se descubre una amenaza. Su desventaja es que únicamente detectan los virus que conocen (o versiones ligeramente modificadas).

Desinfección

Las opciones de desinfección determinan el comportamiento del análisis durante la desinfección de archivos infectados. Hay 3 niveles de desinfección:

Sin desinfección: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de

alerta y permitirá que el usuario seleccione una acción. Este nivel es adecuado para usuarios avanzados que conocen los pasos necesarios en caso de amenaza.

Desinfección normal: el programa intenta desinfectar o eliminar un archivo infectado de manera automática, de acuerdo con una acción predefinida (según el tipo de amenaza). La eliminación y la detección de un archivo infectado se marca mediante una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrece otras acciones que seguir. Lo mismo ocurre cuando no se puede completar una acción predefinida.

Desinfección estricta: el programa desinfecta o elimina todos los archivos infectados. Las únicas excepciones son los archivos del sistema. Si no es posible desinfectar un archivo, se preguntará al usuario qué tipo de acción debe realizarse.

ADVERTENCIA: si un archivo comprimido contiene archivos infectados, se puede tratar de dos maneras: en el modo estándar (Desinfección estándar), se elimina el archivo comprimido completo si todos los archivos que contiene están infectados. En el modo **Desinfección estricta**, el archivo se elimina si contiene al menos un archivo infectado, independientemente del estado de los demás archivos.

IMPORTANTE: si el host Hyper-V se está ejecutando en Windows Server 2008 R2, las opciones **Desinfección normal** y **Desinfección estricta** no son compatibles. El análisis de los discos de la máquina virtual se realiza en el modo de solo lectura, **Sin desinfección**. Sea cual sea el nivel de desinfección seleccionado, el análisis siempre se realiza en el modo de solo lectura.

Exclusiones

Una extensión es una parte del nombre de archivo delimitada por un punto que define el tipo y el contenido del archivo. En este apartado de la configuración de parámetros de ThreatSense es posible definir los tipos de archivos que se desean excluir del análisis.

Otros

Al configurar parámetros del motor ThreatSense para un análisis del ordenador a petición, dispone también de las siguientes opciones en la sección **Otros**:

- **Analizar flujos de datos alternativos (ADS)**: los flujos de datos alternativos utilizados por el sistema de archivos NTFS son asociaciones de carpetas y archivos que no se detectan con técnicas de análisis ordinarias. Muchas amenazas intentan evitar los sistemas de detección haciéndose pasar por flujos de datos alternativos.
- **Ejecutar análisis en segundo plano y con baja prioridad**: cada secuencia de análisis consume una cantidad determinada de recursos del sistema. Si se trabaja con programas cuyo consumo de recursos constituye una carga importante para el sistema, es posible activar el análisis en segundo plano con baja prioridad y reservar los recursos para las aplicaciones.
- **Registrar todos los objetos**: si se selecciona esta opción, el archivo de registro mostrará todos los archivos analizados, incluso los que no están infectados. Por ejemplo, si se detecta una amenaza en un archivo comprimido, en el registro se incluirán también los archivos sin infectar del archivo comprimido.
- **Activar optimización inteligente**: si la opción Optimización inteligente está activada, se utiliza la configuración más óptima para garantizar el nivel de análisis más eficaz y, al mismo tiempo, mantener la máxima velocidad de análisis posible. Los diferentes módulos de protección analizan de forma inteligente, con métodos de análisis distintos y aplicados a tipos de archivo específicos. Si la optimización inteligente está desactivada, solamente se aplica la configuración definida por el usuario en el núcleo ThreatSense de los módulos donde se realiza el análisis.
- **Preservar el último acceso con su fecha y hora**: seleccione esta opción para guardar la hora de acceso original de los archivos analizados, en lugar de actualizarlos (por ejemplo, para utilizar con sistemas de copia de seguridad de datos).

Límites

En la sección Límites se puede especificar el tamaño máximo de los objetos y los niveles de archivos anidados que se analizarán:

Configuración de los objetos

Usar parámetros predeterminados del objeto

- **Tamaño máximo del objeto**: define el tamaño máximo de los objetos que se analizarán. El módulo antivirus analizará solo los objetos que tengan un tamaño menor que el especificado. Esta opción solo deben cambiarla usuarios avanzados que tengan motivos específicos para excluir del análisis objetos más grandes. Valor predeterminado: *ilimitado*.
- **Tiempo máximo de análisis para el objeto (seg.)**: define el tiempo máximo asignado para analizar un objeto. Si se especifica un valor definido por el usuario, el módulo antivirus detendrá el análisis de un objeto cuando se haya agotado el tiempo, independientemente de si el análisis ha finalizado o no. Valor predeterminado: *ilimitado*.

Configuración del análisis de archivos comprimidos

Nivel de anidamiento de archivos: especifica el nivel máximo de análisis de archivos. Valor predeterminado: *10*.

Tamaño máx. de archivo en el archivo comprimido: esta opción permite especificar el tamaño máximo de archivo de los archivos contenidos en archivos comprimidos (una vez extraídos) que se van a analizar. Valor predeterminado: *ilimitado*.

NOTA: no se recomienda cambiar los valores predeterminados; en circunstancias normales, no debería haber motivo para hacerlo.

5.2.6.2.1 Extensiones de archivo excluidas del análisis

Una extensión es una parte del nombre de archivo delimitada por un punto que define el tipo y el contenido del archivo. En esta sección de la configuración de parámetros de ThreatSense, es posible definir los tipos de archivos que se desean analizar.

De forma predeterminada, se analizan todos los archivos. Se puede agregar cualquier extensión a la lista de archivos excluidos del análisis.

A veces es necesario excluir archivos del análisis si, por ejemplo, el análisis de determinados tipos de archivo impide la correcta ejecución del programa que utiliza determinadas extensiones. Por ejemplo, quizás sea aconsejable excluir las extensiones .edb, .eml y .tmp cuando se utilizan servidores Microsoft Exchange.

Con los botones **Agregar** y **Quitar**, puede activar o prohibir el análisis de extensiones de archivo específicas. Para añadir una extensión nueva a la lista, haga clic en Agregar, escriba la extensión en el campo en blanco y, a continuación, haga clic en Aceptar. Seleccione **Introduzca múltiples valores** para añadir varias extensiones de archivos delimitadas por líneas, comas o punto y coma. Si está activada la selección múltiple, las extensiones se mostrarán en la lista. Seleccione una extensión en la lista y haga clic en **Quitar** para eliminarla de la lista. Si desea modificar una extensión seleccionada, haga clic en **Editar**.

No se pueden utilizar los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco sustituye a cualquier cadena de caracteres y el signo de interrogación, a cualquier símbolo.

5.2.6.2.2 Parámetros adicionales de ThreatSense

Parámetros adicionales de ThreatSense para archivos nuevos o modificados: la probabilidad de infección en archivos modificados o recién creados es superior que en los archivos existentes, por eso el programa comprueba estos archivos con parámetros de análisis adicionales. Además de los métodos de análisis basados en firmas habituales, se utiliza la heurística avanzada, que detecta amenazas nuevas antes de que se publique la actualización de la base de firmas de virus. El análisis se realiza también en archivos de autoextracción (.sfx) y empaquetadores en tiempo real (archivos ejecutables comprimidos internamente), no solo en los archivos nuevos. Los archivos se analizan, de forma predeterminada, hasta el 10º nivel de anidamiento; además, se analizan independientemente de su tamaño real. Para modificar la configuración de análisis de archivos comprimidos, desactive la opción **Configuración por defecto para archivos comprimidos**.

Para obtener más información sobre los **empaquetadores en tiempo real**, **archivos comprimidos de autoextracción** y **heurística avanzada**, consulte Configuración de parámetros del motor ThreatSense.

Parámetros adicionales de ThreatSense para los archivos ejecutados: de forma predeterminada, la heurística avanzada no se utiliza cuando se ejecutan archivos. Si esta opción está activada, se recomienda encarecidamente dejar activadas las opciones Optimización inteligente y ESET Live Grid con el fin de mitigar su repercusión en el rendimiento del sistema.

5.2.6.2.3 Niveles de desinfección

La protección en tiempo real tiene tres niveles de desinfección (para acceder a la configuración de niveles de desinfección, haga clic en **Parámetros de ThreatSense** en la sección **Protección del sistema de archivos en tiempo real** y, a continuación, en **Desinfección**).

Sin desinfección: los archivos infectados no se desinfectan automáticamente. El programa mostrará una ventana de alerta y permitirá que el usuario seleccione una acción. Este nivel es adecuado para usuarios avanzados que conocen los pasos necesarios en caso de amenaza.

Desinfección normal: el programa intenta desinfectar o eliminar un archivo infectado de manera automática, de acuerdo con una acción predefinida (según el tipo de amenaza). La eliminación y la detección de un archivo infectado se marca mediante una notificación en la esquina inferior derecha de la pantalla. Si no es posible seleccionar la acción correcta de manera automática, el programa ofrece otras acciones que seguir. Lo mismo ocurre cuando no se puede completar una acción predefinida.

Desinfección estricta: el programa desinfecta o elimina todos los archivos infectados. Las únicas excepciones son los archivos del sistema. Si no es posible desinfectar un archivo, se preguntará al usuario qué tipo de acción debe realizarse.

ADVERTENCIA: si un archivo comprimido contiene archivos infectados, se puede tratar de dos maneras: en el modo estándar (Desinfección estándar), se elimina el archivo comprimido completo si todos los archivos que contiene están infectados. En el modo **Desinfección estricta**, el archivo se elimina si contiene al menos un archivo infectado, independientemente del estado de los demás archivos.

IMPORTANTE: si el host Hyper-V se está ejecutando en Windows Server 2008 R2, las opciones **Desinfección normal** y **Desinfección estricta** no son compatibles. El análisis de los discos de la máquina virtual se realiza en el modo de solo lectura, **Sin desinfección**. Sea cual sea el nivel de desinfección seleccionado, el análisis siempre se realiza en el modo de solo lectura.

5.2.6.2.4 Modificación de la configuración de protección en tiempo real

La protección del sistema de archivos en tiempo real es el componente más importante para mantener un sistema seguro, por lo que debe tener cuidado cuando modifique los parámetros correspondientes. Es aconsejable que los modifique únicamente en casos concretos.

Una vez que se ha instalado ESET Mail Security, se optimiza toda la configuración para proporcionar a los usuarios el máximo nivel de seguridad del sistema. Para restaurar la configuración predeterminada, haga clic en ↩ junto a cada ficha de la ventana (**Configuración avanzada** > **Ordenador** > **Protección del sistema de archivos en tiempo real**).

5.2.6.2.5 Análisis de protección en tiempo real

Para verificar que la protección en tiempo real funciona y detecta virus, utilice el archivo de prueba de eicar.com., un archivo inofensivo detectable por todos los programas antivirus. El archivo fue creado por la compañía EICAR (European Institute for Computer Antivirus Research, Instituto europeo para la investigación de antivirus de ordenador) para probar la funcionalidad de los programas antivirus. Este archivo se puede descargar en http://www.eicar.org/download/eicar.com.

5.2.6.2.6 Qué debo hacer si la protección en tiempo real no funciona

En este capítulo se describen los problemas que pueden surgir cuando se utiliza la protección en tiempo real y cómo resolverlos.

Protección en tiempo real desactivada

Si un usuario desactivó la protección en tiempo real sin darse cuenta, será necesario reactivarla. Para volver a activar la protección en tiempo real, vaya a **Configuración** en la ventana principal del programa y haga clic en **Protección del sistema de archivos en tiempo real**.

Si no se activa al iniciar el sistema, probablemente se deba a que la opción **Iniciar automáticamente la protección del sistema de archivos en tiempo real** no está seleccionada. Para activar esta opción, vaya a Configuración avanzada (**F5**) y haga clic en **Ordenador** > **Protección del sistema de archivos en tiempo real** > **Básico** en la sección **Configuración avanzada**. Asegúrese de que la opción **Iniciar automáticamente la protección del sistema de archivos en tiempo real** esté activada.

Si la protección en tiempo real no detecta ni desinfecta amenazas

Asegúrese de que no tiene instalados otros programas antivirus en el ordenador. Si están activadas dos protecciones en tiempo real al mismo tiempo, estas pueden entrar en conflicto. Recomendamos que desinstale del sistema cualquier otro programa antivirus que haya en el sistema antes de instalar ESET.

La protección en tiempo real no se inicia

Si la protección en tiempo real no se activa al iniciar el sistema (y la opción **Iniciar automáticamente la protección del sistema de archivos en tiempo real** está activada), es posible que se deba a conflictos con otros programas. Para obtener ayuda para resolver este problema, póngase en contacto con el Servicio de atención al cliente de ESET.

5.2.6.2.7 Envío de archivos

Puede especificar cómo se enviarán a ESET los archivos y la información estadística. Seleccione la opción **Mediante administración remota o directamente a ESET** para que los archivos y la información estadística se envíen de todas las formas posibles. Seleccione la opción **Mediante administración remota** para entregar los archivos y las estadísticas al servidor de administración remota, que garantizará su posterior entrega a los laboratorios de ESET. Si se selecciona **Directamente a ESET**, todos los archivos sospechosos y la información estadística se envían a los laboratorios de ESET directamente desde el programa.

Cuando hay archivos pendientes de enviar, el botón **Enviar ahora** está activo. Haga clic en este botón para enviar los archivos y la información estadística inmediatamente.

Seleccione **Activar el registro de sucesos** para crear un registro en el que anotar los envíos de archivos e información estadística.

5.2.6.2.8 Estadísticas

El sistema de alerta temprana ThreatSense.Net recopilará información anónima del ordenador relacionada con amenazas detectadas recientemente. Esta información puede incluir el nombre de la amenaza, la fecha y la hora en que se detectó, la versión del producto de seguridad de ESET, la versión del sistema operativo de su ordenador y la configuración regional. Normalmente, las estadísticas se envían a los servidores de ESET una o dos veces al día.

A continuación, se proporciona un ejemplo de paquete de información estadística enviado:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8
```

Envío de archivos: puede indicar cuándo desea que se envíen los datos estadísticos. Si opta por enviarlos **Lo antes posible**, los datos estadísticos se enviarán en cuanto se creen. Esta configuración es aconsejable si se dispone de una conexión a Internet permanente. Si selecciona la opción **Durante la actualización**, los datos estadísticos se enviarán todos juntos cuando se realice la próxima actualización.

5.2.6.2.9 Archivos sospechosos

La ficha **Archivos sospechosos** le permite configurar el modo de envío de amenazas al laboratorio de ESET para su análisis.

Si encuentra un archivo sospechoso, puede enviarlo a nuestros laboratorios para su análisis. Si resulta ser una aplicación maliciosa, su detección se agregará a la siguiente actualización de la base de firmas de virus.

Puede configurar el envío de archivos para que se realice automáticamente o seleccionar **Avisar antes de enviar** si desea saber qué archivos se envían y confirmar el envío.

Si no desea que se envíe ningún archivo, seleccione la opción **No enviar para su análisis**. La selección de la opción de no enviar archivos no afecta al envío de datos estadísticos, que se configura de forma independiente (consulte la sección Estadísticas).

Envío de archivos: de forma predeterminada, la opción **Tan pronto como sea posible** está seleccionada para que los archivos sospechosos se envíen al laboratorio de amenazas de ESET. Esta acción es aconsejable si se dispone de una conexión a Internet permanente y es posible entregar los archivos sospechosos sin retrasos. Seleccione la opción **Durante** la actualización para que los archivos sospechosos se carguen en ThreatSense.Net durante la próxima actualización.

Filtro de exclusión: esta opción le permite excluir del envío determinados archivos o carpetas. Esta opción puede ser útil, por ejemplo, para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo. Los tipos de archivos más comunes se excluyen de manera predeterminada (.doc, etc.). Si lo desea, puede añadir elementos a la lista de archivos excluidos.

Correo electrónico de contacto: su **Correo electrónico de contacto [opcional]** se puede enviar con cualquier archivo sospechoso y se utilizará para solicitarle información adicional para el análisis, en caso de que sea necesaria. Tenga en cuenta que no recibirá una respuesta de ESET, a no ser que sea necesaria más información.

5.2.7 Análisis del ordenador a petición y análisis Hyper-V

En esta sección se ofrecen opciones para seleccionar parámetros de análisis.

NOTA: este selector de perfiles de análisis se aplica al análisis del ordenador a petición y al análisis Hyper-V.

Perfil seleccionado: un conjunto determinado de parámetros que utiliza el análisis a petición. Para crear uno nuevo, haga clic en **Editar** junto a **Lista de perfiles**.

Si desea analizar un objeto específico, puede hacer clic en **Editar** junto a **Objetos del análisis** y seleccionar una opción en el menú desplegable o elegir objetos específicos de la estructura de carpetas (árbol).

En la ventana de objetos del análisis puede definir los objetos (memoria, unidades, sectores, archivos y carpetas) que se deben analizar para buscar amenazas. Seleccione los objetos en la estructura de árbol, que incluye todos los dispositivos disponibles en el ordenador. En el menú desplegable **Objetos del análisis** puede seleccionar objetos predefinidos para el análisis.

- **Por configuración de perfil**: selecciona los objetos definidos en el perfil de análisis seleccionado.
- **Medios extraíbles**: selecciona los disquetes, dispositivos de almacenamiento USB, CD y DVD.
- **Unidades locales**: selecciona todas las unidades de disco del sistema.
- **Unidades de red**: selecciona todas las unidades de red asignadas.
- **Carpetas compartidas**: selecciona todas las carpetas compartidas del servidor local.
- **Sin selección**: cancela todas las selecciones.

Haga clic en Parámetros de ThreatSense para modificar los parámetros de análisis (por ejemplo, los métodos de detección) del análisis a petición del ordenador.

5.2.7.1 Inicio del análisis personalizado y del análisis Hyper-V

Si solo desea analizar un objeto determinado, puede usar la herramienta de análisis personalizado haciendo clic en **Análisis del ordenador** > **Análisis personalizado** y seleccionando una opción en el menú desplegable **Objetos del análisis** o seleccionando objetos específicos en la estructura de carpetas (árbol).

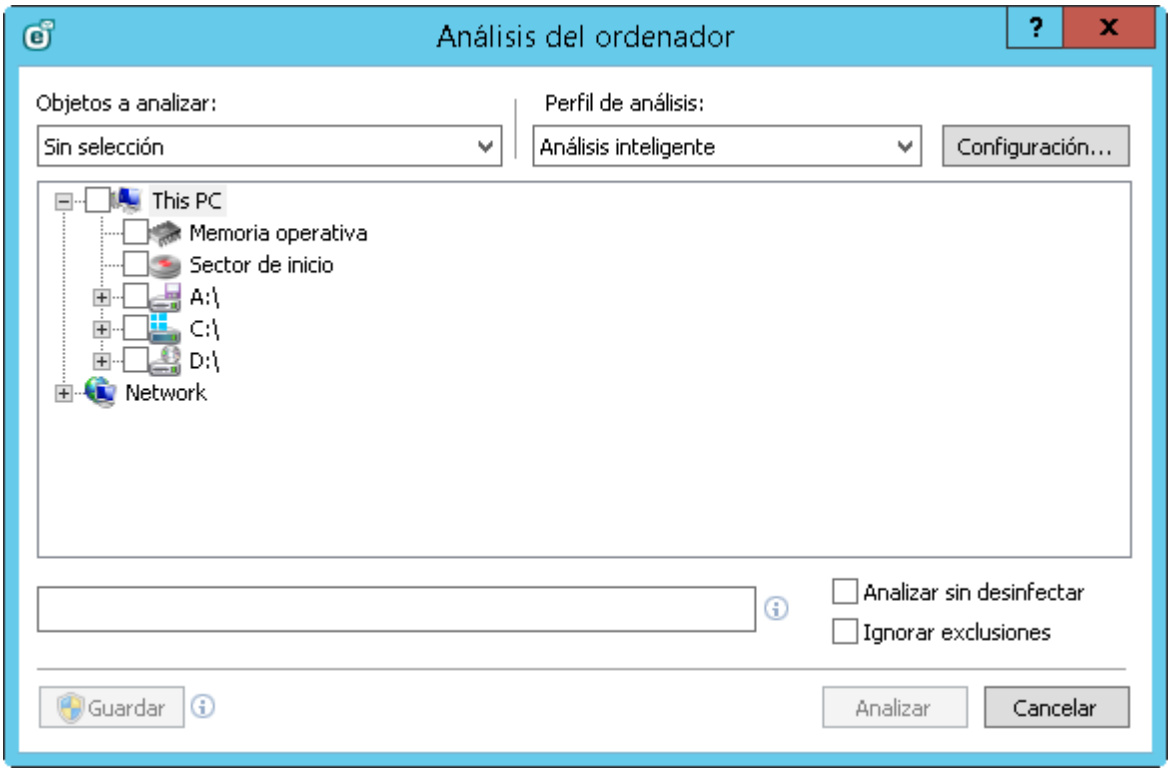
NOTA: este selector de objetos de análisis se aplica al análisis personalizado y al Análisis Hyper-V.

En la ventana de objetos del análisis puede definir los objetos (memoria, unidades, sectores, archivos y carpetas) que se deben analizar para buscar amenazas. Seleccione los objetos en la estructura de árbol, que incluye todos los dispositivos disponibles en el ordenador. En el menú desplegable **Objetos del análisis** puede seleccionar objetos predefinidos para el análisis.

- **Por configuración de perfil**: selecciona los objetos definidos en el perfil de análisis seleccionado.
- **Medios extraíbles**: selecciona los disquetes, dispositivos de almacenamiento USB, CD y DVD.
- **Unidades locales**: selecciona todas las unidades de disco del sistema.
- **Unidades de red**: selecciona todas las unidades de red asignadas.
- **Carpetas compartidas**: selecciona todas las carpetas compartidas del servidor local.
- **Sin selección**: cancela todas las selecciones.

Para acceder rápidamente a un objeto de análisis o agregar directamente un objeto deseado (carpeta o archivos), introdúzcalo en el campo en blanco disponible debajo de la lista de carpetas. Si no se ha seleccionado ningún objeto en la estructura de árbol y el menú **Objetos del análisis** está definido en **Sin selección**, no podrá hacerlo.

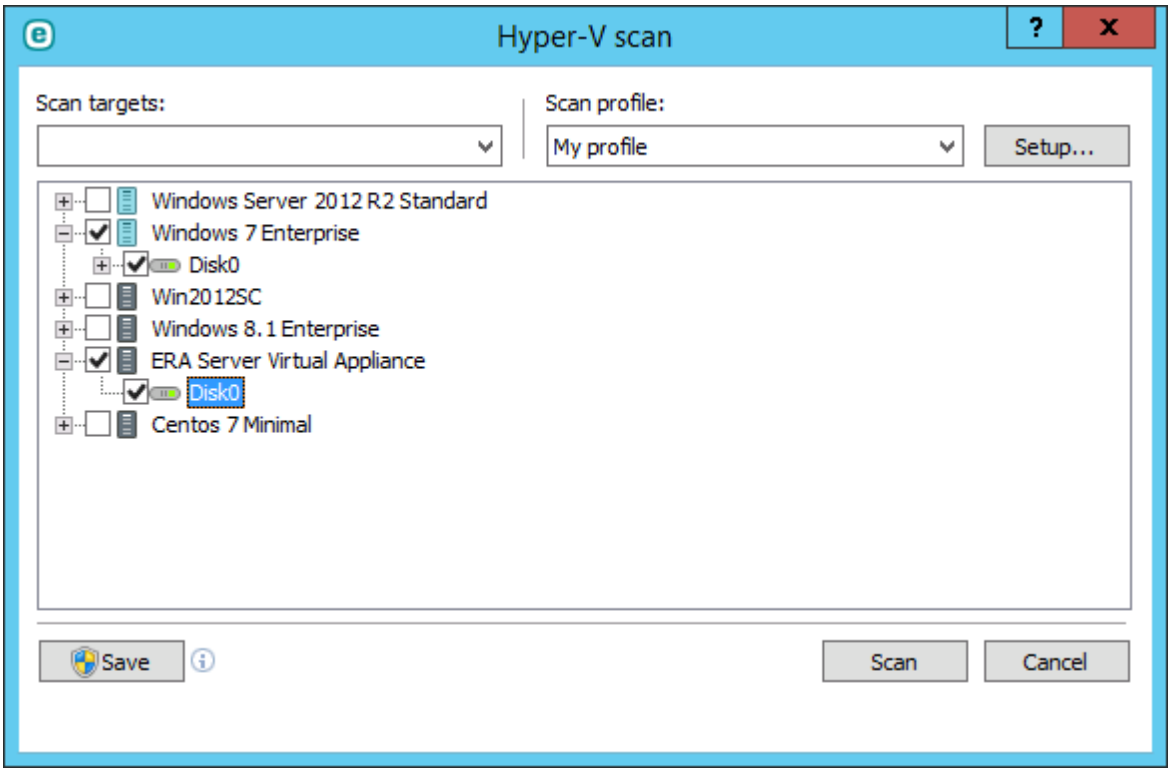
Ventana emergente **Análisis personalizado**:



Si únicamente quiere analizar el sistema, sin realizar acciones de desinfección adicionales, seleccione **Analizar sin desinfectar**. Esta opción resulta útil cuando solo quiere obtener una visión general de si hay elementos infectados y obtener información detallada sobre dichas infecciones, en caso de haber alguna. Además, puede seleccionar uno de los tres niveles de desinfección haciendo clic en **Configuración** > **Parámetros de ThreatSense** > **Desinfección**. La información sobre el análisis se guarda en un registro de análisis.

Cuando selecciona **Ignorar exclusiones**, le permite realizar un análisis ignorando las exclusiones que de otro modo se aplicarían.

Ventana emergente **Análisis Hyper-V** (consulte Análisis Hyper-V para obtener más información):



Puede elegir un perfil en el menú desplegable **Perfil de análisis** que se utilizará para analizar los objetos seleccionados. El perfil predeterminado es **Análisis estándar**. Hay otros dos perfiles de análisis predefinidos llamados **Análisis exhaustivo** y **Análisis del menú contextual**. Estos perfiles de análisis utilizan distintos parámetros del motor ThreatSense. Haga clic en **Configuración...** para configurar en detalle el perfil de análisis elegido en el menú Perfil de análisis. Las opciones disponibles se describen en la sección **Otros** de Configuración de parámetros del motor ThreatSense.

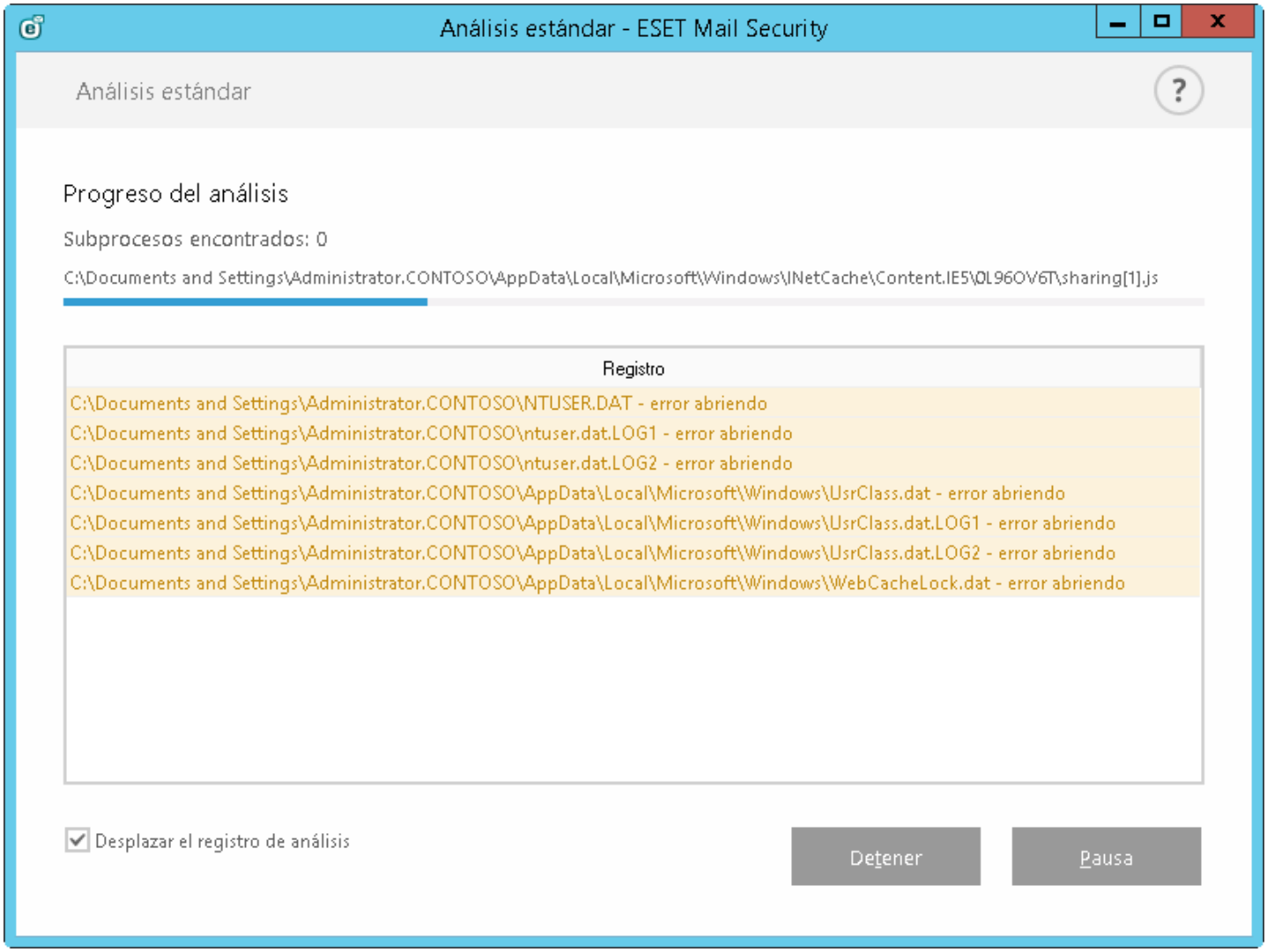
Haga clic en **Guardar** para guardar los cambios realizados en la selección de objetos, incluidas las selecciones realizadas en la estructura de árbol de carpetas.

Haga clic en **Analizar** para ejecutar el análisis con los parámetros personalizados que ha definido.

Analizar como administrador le permite ejecutar el análisis con la cuenta de administrador. Haga clic en esta opción si el usuario actual no tiene privilegios para acceder a los archivos que se deben analizar. Observe que este botón no está disponible si el usuario actual no puede realizar operaciones de UAC como administrador.

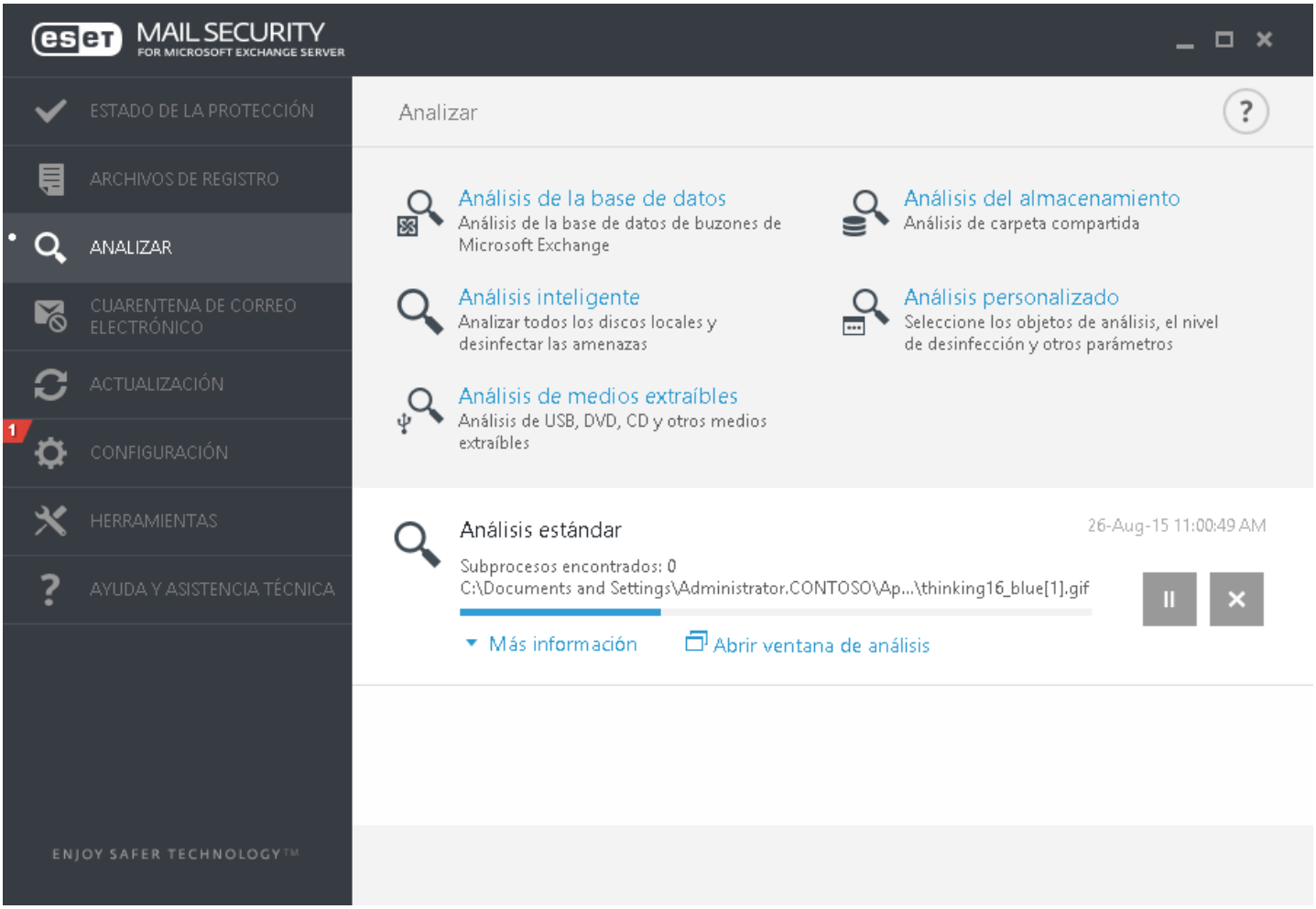
5.2.7.2 Progreso del análisis

En la ventana de progreso del análisis se muestra el estado actual del análisis e información sobre el número de archivos en los que se ha detectado código malicioso.


Análisis estándar - ESET Mail Security
Análisis estándar
Progreso del análisis
Subprocesos encontrados: 0
C:\Documents and Settings\Administrator.CONTOSO\AppData\Local\Microsoft\Windows\INetCache\Content.IE5\0L96OV6T\sharing[1].js
Registro
C:\Documents and Settings\Administrator.CONTOSO\NTUSER.DAT - error abriendo
C:\Documents and Settings\Administrator.CONTOSO\ntuser.dat.LOG1 - error abriendo
C:\Documents and Settings\Administrator.CONTOSO\ntuser.dat.LOG2 - error abriendo
C:\Documents and Settings\Administrator.CONTOSO\AppData\Local\Microsoft\Windows\UsrClass.dat - error abriendo
C:\Documents and Settings\Administrator.CONTOSO\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG1 - error abriendo
C:\Documents and Settings\Administrator.CONTOSO\AppData\Local\Microsoft\Windows\UsrClass.dat.LOG2 - error abriendo
C:\Documents and Settings\Administrator.CONTOSO\AppData\Local\Microsoft\Windows\WebCacheLock.dat - error abriendo
Desplazar el registro de análisis
Detener
Pausa

NOTA: es normal que algunos archivos, como los archivos protegidos con contraseña o que solo utiliza el sistema (por lo general, archivos *pagefile.sys* y determinados archivos de registro), no se puedan analizar.

Progreso del análisis: la barra de progreso muestra el estado de objetos ya analizados en comparación con el porcentaje de objetos pendientes. El estado de progreso del análisis se calcula a partir del número total de objetos incluidos en el análisis.
Objeto: el nombre y la ubicación del objeto que se está analizando.
Amenazas detectadas: muestra el número total de amenazas detectadas durante un análisis.
Pausa: pone el análisis en pausa.
Reanudar: esta opción está visible cuando el progreso del análisis está en pausa. Haga clic en Reanudar para proseguir con el análisis.
Detener: termina el análisis.
Desplazarse por el registro de exploración: si esta opción está activada, el registro de análisis se desplaza automáticamente a medida que se añaden entradas nuevas, de modo que se visualizan las entradas más recientes.



Puede hacer clic en **Más información** durante el proceso de análisis para ver detalles como el **Usuario** que realizó el proceso de análisis desde la interfaz gráfica de usuario, el número de **Objetos analizados** y la **Duración** del análisis. Si se está llevando a cabo el **Análisis de la base de datos** a petición, mostrará el usuario que realizó el análisis, no la Cuenta de análisis de la base de datos real que se está utilizando para establecer la conexión con EWS (Exchange Web Services) durante el proceso de análisis.

5.2.7.3 Administrador de perfiles

El administrador de perfiles se utiliza en dos secciones de ESET Mail Security: en **Análisis de estado inactivo** y en **Actualización**.

Análisis del ordenador

Puede guardar sus parámetros de análisis preferidos para próximas sesiones de análisis. Le recomendamos que cree un perfil diferente (con varios objetos de análisis, métodos de análisis y otros parámetros) para cada uno de los análisis que realice con frecuencia.

Para crear un perfil nuevo, abra la ventana Configuración avanzada (F5) y haga clic en **Ordenador** > **Análisis del**

ordenador a petición y, a continuación, en **Editar** junto a **Lista de perfiles**. En el menú desplegable **Perfil seleccionado** se muestra una lista de los perfiles de análisis disponibles. Si necesita ayuda para crear un perfil de análisis que se adecúe a sus necesidades, consulte el apartado Configuración de parámetros del motor ThreatSense para ver una descripción de los diferentes parámetros de la configuración del análisis.

Ejemplo: supongamos que desea crear su propio perfil de análisis y parte de la configuración del análisis estándar es adecuada; sin embargo, no desea analizar los empaquetadores en tiempo real ni las aplicaciones potencialmente peligrosas y, además, quiere aplicar la opción **Desinfección estricta**. Introduzca el nombre del nuevo perfil en la ventana **Administrador de perfiles** y haga clic en **Agregar**. Seleccione un perfil nuevo en el menú desplegable **Perfil seleccionado**, ajuste los demás parámetros según sus requisitos y haga clic en **Aceptar** para guardar el nuevo perfil.

Actualización

El editor de perfil de la sección de configuración de actualizaciones permite a los usuarios crear nuevos perfiles de actualización. Cree y utilice sus propios perfiles personalizados (es decir, distintos al predeterminado **Mi perfil**) únicamente si su ordenador utiliza varios medios para conectarse a servidores de actualización.

Por ejemplo, un ordenador portátil que normalmente se conecta a un servidor local (Mirror) de la red local, pero descarga las actualizaciones directamente desde los servidores de actualización de ESET cuando se desconecta de la red local (en viajes de negocios) podría utilizar dos perfiles: el primero para conectarse al servidor local y el segundo, a los servidores de ESET. Una vez configurados estos perfiles, seleccione **Herramientas** > **Tareas programadas** y modifique los parámetros de la tarea de actualización. Designe un perfil como principal y el otro como secundario.

Perfil seleccionado: el perfil de actualización utilizado actualmente. Para cambiarlo, seleccione un perfil en el menú desplegable.

Lista de perfiles: cree perfiles de actualización nuevos o edite los actuales.

5.2.7.4 Objetos de análisis

En la ventana de objetos del análisis puede definir los objetos (memoria, unidades, sectores, archivos y carpetas) que se deben analizar para buscar amenazas. Seleccione los objetos en la estructura de árbol, que incluye todos los dispositivos disponibles en el ordenador. En el menú desplegable **Objetos del análisis** puede seleccionar objetos predefinidos para el análisis.

- **Por configuración de perfil**: selecciona los objetos definidos en el perfil de análisis seleccionado.
- **Medios extraíbles**: selecciona los disquetes, dispositivos de almacenamiento USB, CD y DVD.
- **Unidades locales**: selecciona todas las unidades de disco del sistema.
- **Unidades de red**: selecciona todas las unidades de red asignadas.
- **Carpetas compartidas**: selecciona todas las carpetas compartidas del servidor local.
- **Sin selección**: cancela todas las selecciones.

5.2.7.5 Interrupción de un análisis programado

El análisis programado se puede posponer. Defina un valor para la opción **Detener análisis programados en (min)** si desea posponer el análisis del ordenador.

5.2.8 Análisis de estado inactivo

Puede activar el módulo de análisis de estado inactivo en **Configuración avanzada**, bajo **Ordenador** > **Análisis de estado inactivo** > **Básico**. Active el conmutador situado junto a **Activar el análisis de estado inactivo** para activar esta función. Cuando el ordenador se encuentra en estado inactivo, se lleva a cabo un análisis silencioso de todos los discos locales del ordenador.

De forma predeterminada, el análisis de estado inactivo no se ejecutará si el ordenador (portátil) está funcionando con batería. Puede anular este parámetro seleccionando la casilla de verificación situada junto a **Ejecutar aunque el ordenador esté funcionando con la batería** en Configuración avanzada.

Active el conmutador **Activar el registro de sucesos** de la configuración avanzada para guardar un informe del análisis del ordenador en la sección Archivos de registro (en la ventana principal del programa, haga clic en

Herramientas > **Archivos de registro** y seleccione **Análisis del ordenador** en el menú desplegable **Registrar**).

La detección de estado inactivo se ejecutará cuando el ordenador se encuentre en uno de los estados siguientes:

- Pantalla apagada o con protector de pantalla
- Bloqueo de equipo
- Cierre de sesión de usuario

Haga clic en Parámetros de ThreatSense para modificar los parámetros de análisis (por ejemplo, los métodos de detección) del análisis en estado inactivo.

5.2.9 Análisis en el inicio

De forma predeterminada, la comprobación automática de los archivos en el inicio se realizará al iniciar el sistema o durante las actualizaciones la base de firmas de virus. Este análisis está controlado mediante la Configuración y las tareas de Tareas programadas.

Las opciones de análisis en el inicio forman parte de la tarea **Verificación de archivos de inicio del sistema** del Planificador de tareas. Para modificar la configuración del análisis en el inicio, seleccione **Herramientas** > **Tareas programadas**, haga clic en **Verificación automática de los archivos de inicio** y en **Editar**. En el último paso, aparece la ventana Verificación de la ejecución de archivos en el inicio (consulte el siguiente capítulo para obtener más detalles).

Para obtener instrucciones detalladas acerca de la creación y gestión de tareas de Tareas programadas, consulte Creación de tareas nuevas.

5.2.9.1 Verificación de la ejecución de archivos en el inicio

Al crear una tarea programada de comprobación de archivos en el inicio del sistema tiene varias opciones para ajustar los siguientes parámetros:

El menú desplegable **Nivel de análisis** especifica la profundidad del análisis para los archivos que se ejecutan al iniciar el sistema. Los archivos se organizan en orden ascendente de acuerdo con los siguientes criterios:

- **Solo los archivos de uso más frecuente** (se analiza el menor número de archivos)
- **Archivos usados frecuentemente**
- **Archivos usados ocasionalmente**
- **Archivos usados pocas veces**
- **Todos los archivos registrados** (se analiza el mayor número de archivos)

También se incluyen dos grupos específicos de **Nivel de análisis**:

- **Archivos ejecutados antes del inicio de sesión del usuario**: contiene archivos de ubicaciones a las que se puede tener acceso sin que el usuario haya iniciado sesión (incluye casi todas las ubicaciones de inicio como servicios, objetos auxiliares del navegador, notificación del registro de Windows, entradas del Planificador de tareas de Windows, archivos dll conocidos, etc.).
- **Archivos ejecutados tras el inicio de sesión del usuario**: contiene archivos de ubicaciones a las que solo se puede tener acceso cuando el usuario inicia sesión (incluye archivos que solo ejecuta un usuario concreto, generalmente los archivos de *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Las listas de los archivos que se analizan son fijas para cada uno de los grupos anteriores.

Prioridad de análisis: el nivel de prioridad empleado para determinar cuándo se iniciará un análisis:

- **Normal**: con carga media del sistema.
- **Baja**: con poca carga del sistema.
- **Muy baja**: cuando la carga del sistema es la más baja posible.
- **Cuando se encuentra inactivo**: la tarea se ejecutará solo cuando el sistema esté inactivo.

5.2.10 Medios extraíbles

ESET Mail Security permite analizar los medios extraíbles (CD, DVD, USB, etc.) de forma automática. Este módulo le permite analizar un medio insertado. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen medios extraíbles con contenido no solicitado.

Acción que debe efectuarse cuando se insertan medios extraíbles: seleccione la acción predeterminada que se realizará cuando se inserte un medio extraíble en el ordenador (CD, DVD o USB). Si selecciona **Mostrar las opciones de análisis**, se mostrará una ventana en la que puede seleccionar la acción deseada:

- **No analizar**: no se realizará ninguna acción y se cerrará la ventana **Nuevo dispositivo detectado**.
- **Análisis automático del dispositivo**: se realizará un análisis del ordenador a petición del medio extraíble insertado.
- **Mostrar las opciones de análisis**: abre la sección de configuración de medios extraíbles.

Cuando se inserta un medio extraíble aparece la siguiente ventana:

- **Analizar ahora**: activa el análisis del medio extraíble.
- **Analizar más adelante**: el análisis del medio extraíble se pospone.
- **Configuración**: abre la configuración avanzada.
- **Utilizar siempre la opción seleccionada**: cuando se seleccione esta opción, se realizará la misma acción la próxima vez que se introduzca un medio extraíble.

Además, ESET Mail Security presenta funciones de control de dispositivos, lo que le permite definir reglas para el uso de dispositivos externos en un ordenador dado. Encontrará más detalles sobre el control de dispositivos en la sección Control del dispositivo.

5.2.11 Protección de documentos

La característica de protección de documentos analiza los documentos de Microsoft Office antes de que se abran y los archivos descargados automáticamente con Internet Explorer como, por ejemplo, elementos de Microsoft ActiveX. La protección de documentos proporciona un nivel de protección adicional a la protección en tiempo real del sistema de archivos, y se puede desactivar para mejorar el rendimiento en sistemas que no están expuestos a un volumen elevado de documentos de Microsoft Office.

- La opción **Integrar en el sistema** activa el sistema de protección. Si desea modificar esta opción, pulse F5 para abrir la ventana Configuración avanzada y haga clic en **Ordenador** > **Protección de documentos** en el árbol de Configuración avanzada.
- Consulte Parámetros de ThreatSense para obtener más información sobre la configuración de Protección de documentos.

Esta función se activa mediante aplicaciones que utilizan la Antivirus API de Microsoft (por ejemplo, Microsoft Office 2000 y superior, o Microsoft Internet Explorer 5.0 y superior).

5.2.12 HIPS

Solo debe modificar la configuración de HIPS si es un usuario experimentado. Una configuración incorrecta de los parámetros de HIPS puede provocar inestabilidad en el sistema.

El **Sistema de prevención de intrusiones del host** (HIPS) protege el sistema frente a código malicioso o cualquier actividad no deseada que intente menoscabar la seguridad del ordenador. Este sistema combina el análisis avanzado del comportamiento con funciones de detección del filtro de red para controlar los procesos, archivos y claves de registro. HIPS es diferente de la protección del sistema de archivos en tiempo real y no es un cortafuegos, solo supervisa los procesos que se ejecutan dentro del sistema operativo.

Los ajustes del HIPS se puede encontrar en **Configuración avanzada** (F5) > **Ordenador** > **HIPS**. El estado de HIPS (activado/desactivado) se muestra en la ventana principal del programa de ESET Mail Security, en el panel **Configuración** disponible a la derecha de la sección **Ordenador**.

ESET Mail Security tiene una tecnología de *Autodefensa* integrada que impide que el software malicioso dañe o desactive la protección antivirus y antiespía, de modo que el sistema está protegido en todo momento. Los cambios realizados en la configuración de **Activar HIPS** y **Activar la Autodefensa** se aplican después de reiniciar el sistema operativo Windows. También es necesario reiniciar el ordenador para desactivar todo el sistema **HIPS**.

Análisis avanzado de memoria: trabaja conjuntamente con el Bloqueador de exploits para aumentar la protección frente a código malicioso que utiliza los métodos de ofuscación y cifrado para evitar su detección mediante productos de protección frente a este tipo de código. El análisis avanzado de memoria está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

El **Bloqueador de exploits** se ha diseñado para fortificar aquellas aplicaciones que sufren más ataques, como los navegadores de Internet, los lectores de archivos pdf, los clientes de correo electrónico y los componentes de MS Office. El Bloqueador de exploits está activado de forma predeterminada. Puede obtener más información sobre este tipo de protección en el glosario.

El filtrado se puede realizar en cualquiera de los cuatro modos:

- **Modo automático**: las operaciones están activadas, con la excepción de aquellas bloqueadas mediante reglas predefinidas que protegen el sistema.
- **Modo inteligente**: solo se informará al usuario de los sucesos muy sospechosos.
- **Modo interactivo**: el usuario debe confirmar las operaciones.
- **Modo basado en reglas**: las operaciones están bloqueadas.
- **Modo de aprendizaje**: las operaciones están activadas y se crea una regla después de cada operación. Las reglas creadas en este modo se pueden ver en el Editor de reglas, pero su prioridad es inferior a la de las reglas creadas manualmente o en el modo automático. Si selecciona el Modo de aprendizaje en el menú desplegable del modo de filtrado de HIPS, el ajuste El modo de aprendizaje finalizará a las estará disponible. Seleccione el periodo durante el que desea activar el modo de aprendizaje; la duración máxima es de 14 días. Cuando transcurra la duración especificada sele pedirá que modifique las reglas creadas por el HIPS mientras estaba en modo de aprendizaje. También puede elegir un modo de filtrado distinto o posponer la decisión y seguir usando el modo de aprendizaje.

El sistema HIPS supervisa los sucesos del sistema operativo y reacciona de acuerdo con reglas similares a las que utiliza el cortafuegos personal. Haga clic en **Editar** para abrir la ventana de gestión de reglas de HIPS. Aquí puede seleccionar, crear, modificar o eliminar reglas. Encontrará más información sobre la creación de reglas y el funcionamiento de HIPS en el capítulo Editar regla.

Si la acción predeterminada para una regla es Preguntar, se mostrará un cuadro de diálogo cada vez que se desencadene dicha regla. Puede seleccionar entre **Bloquear** y **Permitir** la operación. Si no selecciona una opción en el tiempo indicado, se aplican las reglas para seleccionar la nueva acción.

El cuadro de diálogo permite crear reglas de acuerdo con cualquier nueva acción que detecte HIPS y definir las condiciones en las que se permite o se bloquea dicha acción. Los parámetros exactos se pueden consultar haciendo clic en **Mostrar opciones**. Las reglas creadas con este método se tratan igual que las creadas manualmente, por lo que una regla creada desde un cuadro de diálogo puede ser menos específica que la regla que activó dicho cuadro de diálogo. Esto significa que, después de crear esta regla, la misma operación puede activar la misma ventana.

Recordar temporalmente esta acción para este proceso provoca que se use la acción (**Permitir/Bloquear**) hasta que se cambien las reglas o el modo de filtrado, se actualice el módulo HIPS o se reinicie el sistema. Después de cualquiera de estas tres acciones, las reglas temporales se eliminarán.

5.2.12.1 Reglas de HIPS

En esta ventana se muestra una descripción general de las reglas de HIPS existentes.

Columnas

Regla: nombre de la regla definido por el usuario o seleccionado automáticamente.
Activado: desactive este conmutador si desea conservar la regla en la lista pero no quiere utilizarla.
Acción: la regla especifica la acción (**Permitir**, **Bloquear** o **Preguntar**) que debe realizarse cuando se cumplen las condiciones.
Orígenes: la regla solo se utilizará si una aplicación activa el suceso.
Objetos: la regla solo se usará si la operación está relacionada con un archivo, una aplicación o una entrada del registro específicos.
Registro: si activa esta opción, la información acerca de esta regla se anotará en el registro de HIPS.
Notificar: cuando se activa un suceso se abre una ventana emergente pequeña en la esquina inferior derecha.

Elementos de control

Agregar: crea una nueva regla.
Editar: le permite modificar las entradas seleccionadas.
Quitar: elimina las entradas seleccionadas.

5.2.12.1.1 Configuración de regla de HIPS

- **Nombre de la regla**: nombre de la regla definido por el usuario o seleccionado automáticamente.
- **Acción**: la regla especifica la acción (**Permitir**, **Bloquear** o **Preguntar**) que debe realizarse cuando se cumplen las condiciones.

Operaciones afectadas: debe seleccionar el tipo de operación a la que se aplicará la regla. La regla solo se utilizará para este tipo de operación y para el destino seleccionado.
- **Archivos**: la regla solo se utilizará si la operación está relacionada con este objetivo. Seleccione Archivos específicos en el menú desplegable y haga clic en Agregar para agregar nuevos archivos o carpetas, o puede seleccionar Todos los archivos en el menú desplegable para agregar todas las aplicaciones.
- **Aplicaciones**: la regla solo se utilizará si esta aplicación activa el suceso. Seleccione Aplicaciones específicas en el menú desplegable y haga clic en Agregar para agregar nuevos archivos o carpetas, o puede seleccionar Todas las aplicaciones en el menú desplegable para agregar todas las aplicaciones.
- **Entradas del registro**: la regla solo se utilizará si la operación está relacionada con este objetivo. Seleccione Entradas especificadas en el menú desplegable y haga clic en Agregar para agregar nuevos archivos o carpetas, o puede seleccionar Todas las entradas en el menú desplegable para agregar todas las aplicaciones.
- **Activado**: desactive este conmutador si desea conservar la regla en la lista pero no quiere utilizarla.
- **Registro**: si activa esta opción, la información acerca de esta regla se anotará en el registro de HIPS.
- **Notificar al usuario**: cuando se activa un suceso se abre una ventana emergente pequeña en la esquina inferior derecha.

La regla consta de partes que describen las condiciones que activan esta regla:

Aplicaciones de origen: la regla solo se utilizará si esta aplicación activa el suceso.Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.
Archivos: la regla solo se utilizará si la operación está relacionada con este objeto. Seleccione **Archivos específicos** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todos los archivos** en el menú desplegable para agregar todas las aplicaciones.
Aplicaciones: la regla solo se utilizará si la operación está relacionada con este objeto. Seleccione **Aplicaciones específicas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todas las aplicaciones** en el menú desplegable para agregar todas las aplicaciones.
Entradas del registro: la regla solo se utilizará si la operación está relacionada con este objetivo. Seleccione **Entradas especificadas** en el menú desplegable y haga clic en **Agregar** para agregar nuevos archivos o carpetas, o puede seleccionar **Todas las entradas** en el menú desplegable para agregar todas las aplicaciones.

Descripción de las operaciones importantes:

Operaciones del archivo

- **Eliminar archivo**: la aplicación solicita permiso para eliminar el archivo objetivo.
- **Escribir en archivo**: la aplicación solicita permiso para escribir en el archivo objetivo.
- **Acceso directo al disco**: la aplicación está intentando realizar una operación de lectura o escritura en el disco de una forma no convencional que burlará los procedimientos habituales de Windows. Esto puede provocar la modificación de archivos sin la aplicación de las reglas correspondientes. Esta operación puede estar provocada por un código malicioso que intente evadir el sistema de detección, un software de copia de seguridad que intente realizar una copia exacta de un disco o un gestor de particiones que intente reorganizar los volúmenes del disco.
- **Instalar enlace global**: hace referencia a la invocación de la función SetWindowsHookEx desde la biblioteca MSDN.
- **Cargar controlador**: instalación y carga de controladores en el sistema.

Operaciones de la aplicación

- **Depurar otra aplicación**: conexión de un depurador al proceso. Durante el proceso de depuración de una aplicación es posible ver y modificar muchos aspectos de su comportamiento, así como acceder a sus datos.
- **Interceptar sucesos de otra aplicación**: la aplicación de origen está intentando capturar sucesos dirigidos a una aplicación concreta (por ejemplo un registrador de pulsaciones que intenta capturar sucesos del navegador).
- **Finalizar/suspender otra aplicación**: suspende, reanuda o termina un proceso (se puede acceder a esta operación directamente desde el Process Explorer o el panel Procesos).
- **Iniciar una aplicación nueva**: inicia aplicaciones o procesos nuevos.
- **Modificar el estado de otra aplicación**: la aplicación de origen está intentando escribir en la memoria de la aplicación de destino o ejecutar código en su nombre. Esta función puede ser de utilidad para proteger una aplicación fundamental mediante su configuración como aplicación de destino en una regla que bloquee el uso de esta operación.

Operaciones del registro

- **Modificar la configuración del inicio**: cambios realizados en la configuración que definan las aplicaciones que se ejecutarán al iniciar Windows. Estos cambios se pueden buscar, por ejemplo, buscando la clave Run en el Registro de Windows.
- **Eliminar del registro**: elimina una clave del registro o su valor.
- **Cambiar el nombre de la clave del registro**: cambia el nombre de las claves del registro.
- **Modificar el registro**: crea valores nuevos para las claves del registro, modifica los valores existentes, mueve los datos en el árbol de la base de datos o configura los permisos de usuarios y grupos en las claves del registro.

NOTA: puede utilizar comodines, con determinadas restricciones, para especificar un destino. En las rutas de acceso al registro se puede utilizar el símbolo * (asterisco) en vez de una clave determinada. Por ejemplo *HKEY_USERS*\software* puede significar *HKEY_USER\.default\software*, pero no *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*. *HKEY_LOCAL_MACHINE\system\ControlSet** no es una ruta válida para la clave del registro. Una ruta de la clave del registro que tenga * incluye "esta ruta, o cualquier ruta de cualquier nivel después del símbolo". Este es el único uso posible de los comodines en los destinos. Primero se evalúa la

parte específica de una ruta de acceso y, después, la ruta que sigue al comodín (*).

Si crea una regla muy genérica se mostrará una advertencia sobre este tipo de regla.

5.2.12.2 Configuración avanzada

Las opciones siguientes son útiles para depurar y analizar el comportamiento de una aplicación:

Controladores con carga siempre autorizada: los controladores seleccionados pueden cargarse siempre sea cual sea el modo de filtrado configurado, a menos que la regla del usuario los bloquee de forma explícita.

Registrar todas las operaciones bloqueadas: todas las operaciones bloqueadas se anotarán en el registro de HIPS.

Notificar cuando se produzcan cambios en las aplicaciones de inicio: muestra una notificación en el escritorio cada vez que se agrega o se elimina una aplicación del inicio del sistema.

Consulte nuestro artículo de la base de conocimiento para ver una versión actualizada de esta página de ayuda.

5.2.12.2.1 Controladores con carga siempre autorizada

Los controladores que aparezcan en esta lista podrán cargarse siempre, sea cual sea el modo de filtrado de HIPS, a menos que una regla del usuario los bloquee de forma específica.

Agregar: agrega un nuevo controlador.
Editar: permite modificar la ruta de acceso del controlador seleccionado.
Quitar: quita un controlador de la lista.
Restablecer: carga de nuevo una serie de controladores del sistema.

NOTA: haga clic en **Restablecer** si no desea incluir los controladores que ha agregado manualmente. Esto puede resultar útil si ha agregado varios controladores y no puede eliminarlos de la lista manualmente.

5.3 Actualizar

Las opciones de configuración de actualizaciones están disponibles en el árbol de **Configuración avanzada** (F5), en **Actualización** > **General**. En esta sección se especifica la información del origen de la actualización, como los servidores de actualización utilizados y sus datos de autenticación.

General

El perfil de actualización que se está utilizando se muestra en el menú desplegable **Perfil seleccionado**. Para crear un perfil nuevo, haga clic en **Editar** junto a **Lista de perfiles**, introduzca su **Nombre de perfil** y, a continuación, haga clic en **Agregar**.

Si tiene problemas con la actualización, haga clic en el botón **Borrar** para vaciar la caché de actualización temporal.

Alertas de base de firmas de virus no actualizada

Establecer antigüedad máxima de la base de firmas automáticamente: permite establecer el tiempo (en días) máximo tras el cual la base de firmas de virus se considerará desactualizada. El valor predeterminado es 7.

- **Revertir**

Si sospecha que una nueva actualización de la base de firmas de virus o de los módulos del programa puede ser inestable o estar dañada, puede revertir a la versión anterior y desactivar las actualizaciones durante un periodo de tiempo definido. También puede activar actualizaciones desactivadas con anterioridad si las había pospuesto indefinidamente.

ESET Mail Security registra instantáneas de la base de firmas de virus y los módulos del programa para usarlas con la función de *reversión*. Para crear instantáneas de la base de firmas de virus, deje activado el conmutador **Crear instantáneas de archivos de actualización**. El campo **Número de instantáneas almacenadas localmente** define el número de instantáneas de la base de firmas de virus anteriores que se guardan.

Si hace clic en **Revertir** (**Configuración avanzada** (F5) > **Actualización** > **General**), deberá seleccionar un intervalo de tiempo en el menú desplegable que representa el periodo de tiempo durante el que estarán interrumpidas las actualizaciones de la base de firmas de virus y del módulo del programa.

Para que las actualizaciones se descarguen correctamente, es esencial cumplimentar correctamente todos los parámetros de actualización. Si utiliza un cortafuegos, asegúrese de que su programa de ESET goza de permiso para comunicarse con Internet (por ejemplo, comunicación HTTP).

De forma predeterminada, el menú **Tipo de actualización** (situado en **Básico**) está definido en **Actualización normal** para garantizar que todos los archivos de actualización se descarguen automáticamente del servidor de ESET cuando la carga de red sea menor.

Básico

Desactivar la notificación de la actualización correcta: desactiva la notificación de la bandeja del sistema en la esquina inferior derecha de la pantalla. Selecciónela si está ejecutando un juego o una aplicación a pantalla completa. Tenga en cuenta que el modo de presentación desactiva todas las notificaciones.

El menú **Servidor de actualización** está establecido en AUTOSELECT de forma predeterminada. El servidor de actualización es la ubicación donde se almacenan las actualizaciones. Si utiliza un servidor ESET, le recomendamos que deje seleccionada la opción predeterminada. Si está utilizando un servidor de actualizaciones personalizado y desea volver al predeterminado, escriba **AUTOSELECT**. ESET Mail Security elegirá automáticamente los servidores de actualización de ESET.

Cuando se utiliza un servidor local HTTP, también conocido como Mirror, el servidor de actualización debe configurarse de la forma siguiente:
http://nombre_del_ordenador_o_su_dirección_IP:2221

Cuando se utiliza un servidor local HTTP con SSL, el servidor de actualización debe configurarse de la forma siguiente:
https://nombre_del_ordenador_o_su_dirección_IP:2221

Cuando se utiliza una carpeta local compartida, el servidor de actualización debe configurarse de la forma siguiente:
\\nombre_o_dirección_IP_ordenador\carpeta_compartida

- **Actualización desde el servidor Mirror**

La autenticación de los servidores de actualización se basa en la **clave de licencia** generada y enviada tras la compra. Si utiliza un servidor Mirror local, puede definir credenciales para que los clientes inicien sesión en dicho servidor antes de recibir actualizaciones. De forma predeterminada, no se requiere ningún tipo de verificación y los campos **Nombre de usuario** y **Contraseña** se dejan en blanco.

5.3.1 Reversión de actualización

Si hace clic en **Revertir** (**Configuración avanzada** (F5) > **Actualización** > **Perfil**), deberá seleccionar un intervalo de tiempo en el menú desplegable que representa el periodo de tiempo durante el que estarán interrumpidas las actualizaciones de la base de firmas de virus y del módulo del programa.

Seleccione **Hasta que se revoque** si desea posponer las actualizaciones periódicas indefinidamente hasta que restaure la funcionalidad manualmente. Como esto representa un riesgo de seguridad potencial, no recomendamos que se seleccione esta opción.

La versión de la base de firmas de virus se degrada a la más antigua disponible y se almacena como instantánea en el sistema de archivos del ordenador local.

Ejemplo: supongamos que el número 10646 es la versión más reciente de la base de firmas de virus. 10645 y 10643 se almacenan como instantáneas de base de firmas de virus. Observe que 10644 no está disponible porque, por ejemplo, el ordenador estuvo apagado y había disponible una actualización más reciente antes de que se descargara 10644. Si se ha definido 2 en el campo **Número de instantáneas almacenadas localmente** y hace clic en **Revertir**, la base de firmas de virus (incluidos los módulos del programa) se restaurará a la versión número 10643. Este proceso puede tardar bastante. Compruebe si la versión de la base de firmas de virus se ha degradado en la ventana principal del programa de ESET Mail Security en la sección Actualización.

5.3.2 Tipo de actualización

La ficha **Modo de actualización** contiene las opciones relacionadas con la actualización de componentes del programa. Este programa le permite predefinir su comportamiento cuando está disponible una nueva actualización de componentes del programa.

Las actualizaciones de componentes del programa presentan nuevas características, o realizan cambios en las características que ya existen de versiones anteriores. Se puede realizar de manera automática, sin la intervención del usuario, o configurar de modo que reciba una notificación de dicha actualización. Después de instalar una actualización de componentes del programa, puede que sea necesario reiniciar el ordenador. En la sección **Actualización de componentes del programa** hay tres opciones disponibles:

- **Avisar antes de descargar los componentes del programa**: esta es la opción predeterminada. Se le solicitará que confirme o rechace las actualizaciones de componentes del programa cuando estén disponibles.
- **Actualizar siempre los componentes del programa**: se descargará e instalará una actualización de componentes del programa de manera automática. Recuerde que es posible que tenga que reiniciar el ordenador.
- **Nunca actualizar los componentes del programa**: las actualizaciones de componentes del programa no se realizarán. Esta opción es adecuada para las instalaciones de servidores, dado que normalmente los servidores solo se pueden reiniciar cuando realizan tareas de mantenimiento.

NOTA: la selección de la opción más adecuada depende de la estación de trabajo donde se vaya a aplicar la configuración. Tenga en cuenta que existen ciertas diferencias entre estaciones de trabajo y servidores; por ejemplo, el reinicio automático del servidor tras una actualización del programa podría causar daños graves.

Si está activada la opción **Preguntar antes de descargar actualizaciones**, se mostrará una notificación cuando esté disponible una nueva actualización.

Si el tamaño del archivo de actualización es superior al valor especificado en el campo **Preguntar si un archivo de actualización es mayor de (KB)**, el programa mostrará una notificación.

5.3.3 Servidor Proxy HTTP

Para acceder a las opciones de configuración del servidor proxy de un perfil de actualización concreto, haga clic en **Actualización** en el árbol de **Configuración avanzada** (F5) y, a continuación, en **Proxy HTTP**. Haga clic en el menú desplegable **Modo proxy** y seleccione una de estas tres opciones:

- No usar servidor Proxy
- Conexión a través de un servidor Proxy específico
- Utilizar la configuración predeterminada

Si selecciona la opción **Usar la configuración global del servidor proxy**, se utilizarán las opciones de configuración del servidor proxy ya especificadas en la sección **Herramientas** > **Servidor proxy** del árbol de Configuración avanzada.

Seleccione **No usar servidor proxy** para especificar que no se utilice ningún servidor proxy para actualizar ESET Mail Security.

La opción **Conexión a través de un servidor proxy** debe seleccionarse si:

- Para actualizar ESET Mail Security, es necesario utilizar un servidor proxy diferente al especificado en la configuración global (**Herramientas** > **Servidor proxy**). En este caso, será necesario especificar la configuración aquí: Dirección del **Servidor proxy**, **Puerto** de comunicación (3128 de forma predeterminada), **Nombre de usuario** y **Contraseña** del servidor proxy, si es necesario.
- La configuración del servidor proxy no se ha definido globalmente, pero ESET Mail Security se conecta a un servidor proxy para las actualizaciones.
- El ordenador se conecta a Internet mediante un servidor proxy. La configuración se toma de Internet Explorer durante la instalación del programa; no obstante, si esta cambia (por ejemplo, al cambiar de proveedor de Internet), compruebe que la configuración del servidor proxy HTTP es correcta en esta ventana. De lo contrario, el programa no se podrá conectar a los servidores de actualización.

La configuración predeterminada del servidor proxy es **Usar la configuración global del servidor proxy**.

NOTA: los datos de autenticación, como el **Nombre de usuario** y la **Contraseña** sirven para acceder al servidor proxy. Rellene estos campos únicamente si es necesario introducir un nombre de usuario y una contraseña. Tenga en cuenta que en estos campos no debe introducir su contraseña y nombre de usuario de ESET Mail Security, que únicamente debe proporcionar si sabe que es necesaria una contraseña para acceder a Internet a través de un servidor proxy.

5.3.4 Conectarse a la LAN como

Para realizar una actualización desde un servidor local con una versión del sistema operativo Windows NT, es necesario autenticar todas las conexiones de red de forma predeterminada.

Para configurar una cuenta de este tipo, seleccione en el menú desplegable **Tipo de usuario local**:

- **Cuenta del sistema (predeterminado)**
- **Usuario actual**
- **Usuario especificado**

Seleccione **Cuenta de sistema (predeterminado)** para utilizar la cuenta del sistema para la autenticación. Normalmente no se realiza ningún proceso de autenticación si no se proporcionan datos en la sección de configuración de actualizaciones.

Para garantizar que el programa se autentique con la cuenta de un usuario registrado actualmente, seleccione **Usuario actual**. El inconveniente de esta solución es que el programa no se puede conectar al servidor de actualizaciones si no hay ningún usuario registrado.

Seleccione **Especificar usuario** si desea que el programa utilice una cuenta de usuario específica para la autenticación. Utilice este método cuando falle la conexión predeterminada con la cuenta del sistema. Recuerde que la cuenta del usuario especificado debe tener acceso al directorio de archivos actualizados del servidor local. De lo contrario, el programa no podrá establecer ninguna conexión ni descargar las actualizaciones.

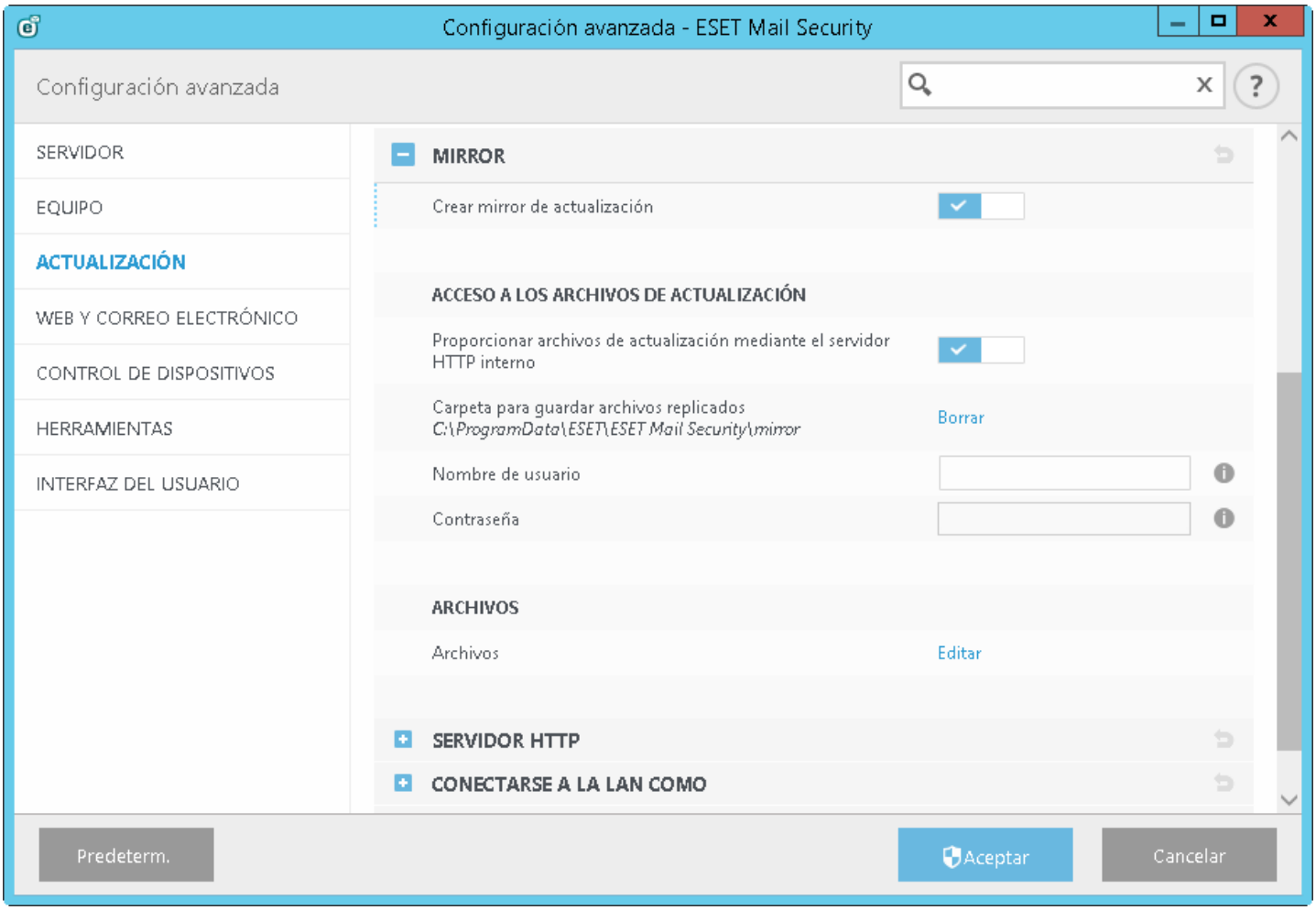
ADVERTENCIA: Cuando se selecciona **Usuario actual** o **Especificar usuario**, puede producirse un error al cambiar la identidad del programa para el usuario deseado. Por este motivo, se recomienda que introduzca los datos de autenticación de la red local en la sección principal de configuración de actualizaciones, donde los datos de autenticación se deben introducir de la forma siguiente: *nombre_dominio**usuario* (si es un grupo de trabajo, escriba *nombre_grupo de trabajo**nombre*) y la contraseña. Cuando se actualiza desde la versión HTTP del servidor local, no es necesaria ninguna autenticación.

Seleccione **Desconectar del servidor tras la actualización** para forzar la desconexión si una conexión al servidor permanece inactiva incluso después de descargar las actualizaciones.

5.3.5 Mirror

ESET Mail Security le permite crear copias de los archivos de actualización, que puede utilizar para actualizar otras estaciones de trabajo de la red. El uso de un *"mirror"*: es conveniente realizar una copia de los archivos de actualización del entorno de red local, dado que no necesitan descargarse del servidor de actualización del proveedor varias veces ni que los descarguen todas las estaciones de trabajo. Las actualizaciones se descargan de manera centralizada en el servidor Repositorio local y, después, se distribuyen a todas las estaciones de trabajo para así evitar el riesgo de sobrecargar el tráfico de red. La actualización de estaciones de trabajo cliente desde un servidor Mirror optimiza el equilibrio de carga de la red y ahorra ancho de banda de la conexión a Internet.

Las opciones de configuración del servidor Mirror local están disponibles en la sección Configuración avanzada, dentro de **Actualización**. Para acceder a esta sección pulse F5 para ir a Configuración avanzada, haga clic en **Actualización** y seleccione la ficha **Mirror**.



Si desea crear un mirror en una estación de trabajo cliente, active la opción **Crear mirror de actualización**. Al activar dicha opción se activan otras opciones de configuración del Mirror, como la forma de acceder a los archivos actualizados y la ruta de actualización de los archivos replicados.

Acceso a los archivos de actualización

Proporcionar archivos de actualización mediante el servidor HTTP interno: si se activa esta opción, es posible acceder a los archivos de actualización a través de HTTP sin necesidad de credenciales.

NOTA: para usar el servidor HTTP en Windows XP se necesita el Service Pack 2 o superior.

En el apartado Actualización desde el servidor Mirror se describen exhaustivamente los métodos de acceso al servidor Mirror. Existen dos métodos básicos para acceder al servidor Mirror: la carpeta que contiene los archivos de actualización se puede presentar como una carpeta de red compartida o los clientes pueden acceder al Mirror situado en un servidor HTTP.

La carpeta destinada a almacenar los archivos de actualización para el servidor Mirror se define en la sección **Carpeta**

para guardar archivos replicados. Haga clic en **Carpeta** para buscar una carpeta en el ordenador local o en la carpeta de red compartida. Si es necesaria una autorización para la carpeta especificada, deberá especificar los datos de autenticación en los campos **Nombre de usuario** y **Contraseña**. Si la carpeta de destino seleccionada se encuentra en un disco de red que ejecuta los sistemas operativos Windows NT, 2000 o XP, el nombre de usuario y la contraseña especificados deben contar con privilegios de escritura para la carpeta seleccionada. El nombre de usuario y la contraseña deben introducirse con el formato *Dominio/Usuario* o *Grupo de trabajo/Usuario*. No olvide que debe introducir las contraseñas correspondientes.

Archivos: durante la configuración del servidor Mirror puede especificar las versiones de idioma de las actualizaciones que desea descargar. Los idiomas seleccionados deben ser compatibles con el servidor Mirror configurado por el usuario.

Servidor HTTP

Puerto de servidor: el puerto de servidor predeterminado es el 2221.

Autenticación: define el método de autenticación utilizado para acceder a los archivos de actualización. Están disponibles las opciones siguientes: **Ninguna**, **Básica** y **NTLM**. Seleccione **Básica** para utilizar la codificación base64 con la autenticación básica de nombre de usuario y contraseña. La opción **NTLM** proporciona la codificación a través de un método seguro. Para la autenticación se utilizará el usuario creado en la estación de trabajo que comparte los archivos actualizados. La configuración predeterminada es **NINGUNA** y concede acceso a los archivos de actualización sin necesidad de autenticación.

Si desea ejecutar el servidor HTTP con compatibilidad HTTPS (SSL), agregue el **archivo de cadena de certificados** o genere un certificado autofirmado. Están disponibles los siguientes tipos de certificado: ASN, PEM y PFX. Para una mayor seguridad, puede utilizar el protocolo HTTPS para descargar los archivos de actualización. Resulta casi imposible hacer un seguimiento de las transferencias de datos y credenciales de inicio de sesión utilizando este protocolo. La opción **Tipo de clave privada** está establecida de forma predeterminada en **Integrada** (y, por lo tanto, la opción **Archivo de clave privada** está desactivada de forma predeterminada). Esto significa que la clave privada forma parte del archivo de cadena de certificados seleccionado.

Conectarse a la LAN como

Tipo de usuario local: las opciones **Cuenta del sistema (predeterminado)**, **Usuario actual** y **Usuario especificado** se mostrarán en los menús desplegables correspondientes. Los campos **Nombre de usuario** y **Contraseña** son opcionales. Consulte Conectarse a la LAN como.

Seleccione **Desconectar del servidor tras la actualización** para forzar la desconexión si una conexión al servidor permanece inactiva incluso después de descargar las actualizaciones.

Actualización de componentes del programa

Actualizar componentes automáticamente: permite instalar características nuevas y actualizaciones de las características existentes. La actualización se puede realizar de manera automática, sin la intervención del usuario, o configurar de modo que este reciba una notificación. Después de instalar una actualización de componentes del programa, puede que sea necesario reiniciar el ordenador.

Actualizar componentes ahora: actualiza los componentes del programa a la versión más reciente.

5.3.5.1 Actualización desde el servidor Mirror

El servidor Mirror es básicamente un repositorio en el que los clientes pueden descargar los archivos de actualización. Existen dos métodos de configuración básicos de este tipo de servidor. La carpeta que contiene los archivos de actualización puede presentarse como una carpeta de red compartida o como un servidor HTTP.

Acceso al servidor Mirror mediante un servidor HTTP interno

Esta es la configuración predeterminada, especificada en la configuración predefinida del programa. Para permitir el acceso al Mirror mediante el servidor HTTP, vaya a **Configuración avanzada** > **Actualización** > **Mirror** y seleccione **Crear mirror de actualización**.

En la sección **Servidor HTTP** de la ficha **Mirror**, puede especificar el **Puerto del servidor** donde el servidor HTTP estará a la escucha, así como el tipo de **autenticación** que utiliza el servidor HTTP. El valor predeterminado del puerto del servidor es **2221**. La opción **Autenticación** define el método de autenticación utilizado para acceder a los archivos de actualización. Están disponibles las opciones siguientes: **Ninguna**, **Básica** y **NTLM**.

- Seleccione **Básica** para utilizar la codificación base64 con la autenticación básica de nombre de usuario y contraseña.
- La opción **NTLM** proporciona la codificación a través de un método seguro. Para la autenticación se utilizará el usuario creado en la estación de trabajo que comparte los archivos actualizados.
- La configuración predeterminada es **Ninguna** y concede acceso a los archivos de actualización sin necesidad de autenticación.

ADVERTENCIA: si desea permitir el acceso a los archivos de actualización a través del servidor HTTP, la carpeta Mirror debe encontrarse en el mismo ordenador que la instancia de ESET Mail Security que vaya a crearla.

SSL para el servidor HTTP

Si desea ejecutar el servidor HTTP con compatibilidad HTTPS (SSL), agregue el **archivo de cadena de certificados** o genere un certificado autofirmado. Están disponibles los siguientes tipos de certificado: **PEM, PFX** y **ASN**. Para una mayor seguridad, puede utilizar el protocolo HTTPS para descargar los archivos de actualización. Resulta casi imposible hacer un seguimiento de las transferencias de datos y credenciales de inicio de sesión utilizando este protocolo. La opción **Tipo de clave privada** está establecida en **Integrada** de forma predeterminada, lo que significa que la clave privada forma parte del archivo de cadena de certificados seleccionado.

NOTA: si se realizan varios intentos sin éxito de actualizar la base de firmas de virus desde el servidor Mirror, en el panel Actualización del menú principal aparecerá el error **El nombre de usuario o la contraseña no son válidos**. Le recomendamos que acceda a **Configuración avanzada** > **Actualización** > **Mirror** y compruebe si el nombre de usuario y la contraseña son correctos. Este error suele estar provocado por la introducción incorrecta de los datos de autenticación.

Una vez que haya configurado su servidor Mirror, debe agregar el nuevo servidor de actualización a las estaciones de trabajo cliente. Para hacerlo, siga estos pasos:

- Acceda a **Configuración** (F5) y haga clic en **Actualización** > **Básico**.
- Desactive **Elegir automáticamente** y agregue un servidor nuevo al campo **Servidor de actualización** con uno de los siguientes formatos:
  http://dirección_IP_de_su_servidor:2221
  https://dirección_IP_de_su_servidor:2221 (si se utiliza SSL)

Acceso al servidor Mirror mediante el uso compartido del sistema

En primer lugar, es necesario crear una carpeta compartida en un dispositivo local o de red. A la hora de crear la carpeta para el mirror, es necesario proporcionar acceso de *"escritura"* al usuario que va a guardar los archivos en la carpeta y acceso de *"lectura"* a todos los usuarios que vayan a actualizar ESET Mail Security desde la carpeta Mirror.

A continuación, configure el acceso al servidor Mirror en la sección **Configuración avanzada** > **Actualización** > **Mirror** mediante la desactivación de la opción **Proporcionar archivos de actualización mediante el servidor HTTP interno**. Esta opción se activa, de forma predeterminada, en el paquete de instalación del programa.

Si la carpeta compartida se encuentra en otro ordenador de la red, debe especificar los datos de autenticación para

acceder al otro ordenador. Para especificar los datos de autenticación, abra **Configuración avanzada** (F5) de ESET Mail Security y haga clic en la sección **Actualización** > **Conectarse a la LAN como**. Esta configuración es la misma que se aplica a las actualizaciones, tal como se describe en la sección Conectarse a la LAN como.

Cuando haya terminado de configurar el servidor Mirror, en las estaciones de trabajo cliente, siga los pasos que se indican a continuación para establecer *UNC**RUTA* como servidor de actualización:

1. Abra la **Configuración avanzada** de ESET Mail Security y haga clic en **Actualización** > **Básico**.
2. Haga clic en el campo **Servidor de actualización** y utilice el formato *UNC**RUTA* para agregar un nuevo servidor.

NOTA: para que las actualizaciones funcionen correctamente es necesario especificar la ruta a la carpeta Mirror como una ruta UNC. Es posible que las actualizaciones de las unidades asignadas no funcionen.

La última sección controla los componentes del programa (PCU). De forma predeterminada, los componentes del programa descargados se preparan para copiarse en el Repositorio local. Si la opción **Actualización de componentes del programa** está activada, no es necesario hacer clic en **Actualizar** porque los archivos se copian en el servidor Repositorio local automáticamente cuando se encuentran disponibles. Consulte Tipo de actualización para obtener más información acerca de las actualizaciones de los componentes del programa.

5.3.5.2 Archivos replicados

Muestra una lista de los archivos de componentes del programa disponibles y localizados.

5.3.5.3 Resolución de problemas de actualización del Mirror

En la mayoría de los casos, los problemas durante la actualización desde un servidor Mirror se deben a una de estas causas: la especificación incorrecta de las opciones de la carpeta Mirror, la introducción de datos de autenticación no válidos para la carpeta Mirror, la configuración incorrecta de las estaciones de trabajo que intentan descargar archivos de actualización del Mirror o una combinación de los motivos anteriores. A continuación, se ofrece información general acerca de los problemas más frecuentes durante la actualización desde el Mirror:

- **ESET Mail Security notifica un error al conectarse al servidor de imagen**: suele deberse a la especificación incorrecta del servidor de actualización (ruta de red a la carpeta Mirror) desde el que se actualizan las descargas de las estaciones de trabajo locales. Para verificar la carpeta, haga clic en el menú **Inicio** de Windows y en **Ejecutar**, introduzca el nombre de la carpeta y haga clic en **Aceptar**. A continuación, debe mostrarse el contenido de la carpeta.
- **ESET Mail Security requiere un nombre de usuario y una contraseña**: probablemente se deba a la presencia de datos de autenticación incorrectos (nombre de usuario y contraseña) en la sección de actualización. El nombre de usuario y la contraseña se utilizan para conceder acceso al servidor de actualización desde el que se actualiza el programa. Asegúrese de que los datos de autenticación son correctos y se introducen en el formato adecuado. Por ejemplo, *Dominio/Nombre de usuario* o *Grupo de trabajo/Nombre de usuario*, más las contraseñas correspondientes. Si "Todos" pueden acceder al servidor Mirror, debe ser consciente de que esto no quiere decir que cualquier usuario tenga acceso. "Todos" no hace referencia a cualquier usuario no autorizado, tan solo significa que todos los usuarios del dominio pueden acceder a la carpeta. Como resultado, si "Todos" pueden acceder a la carpeta, será igualmente necesario introducir un nombre de usuario y una contraseña en la sección de configuración de actualizaciones.
- **ESET Mail Security notifica un error al conectarse al servidor de imagen**: la comunicación del puerto definida para acceder a la versión HTTP del Mirror está bloqueada.

5.3.6 Cómo crear tareas de actualización

Las actualizaciones se pueden activar manualmente al hacer clic en **Actualizar la base de firmas de virus ahora** de la ventana principal que se muestra al hacer clic en **Actualización** en el menú principal.

Las actualizaciones también se pueden ejecutar como tareas programadas. Para configurar una tarea programada, haga clic en **Herramientas** > **Planificador de tareas**. Las siguientes tareas están activadas de forma predeterminada en ESET Mail Security:

- **Actualización automática de rutina**
- **Actualización automática tras conexión de acceso telefónico**
- **Actualización automática después del registro del usuario**

Todas las tareas de actualización se pueden modificar en función de sus necesidades. Además de las tareas de actualización predeterminadas, se pueden crear nuevas tareas de actualización con una configuración definida por el usuario. Para obtener más información acerca de la creación y la configuración de tareas de actualización, consulte la sección Tareas programadas de este manual.

5.4 Web y correo electrónico

En la sección **Internet y correo electrónico** se puede configurar la Protección del cliente de correo electrónico, proteger las comunicaciones por Internet con la Protección del tráfico de Internet y controlar los protocolos de Internet mediante la configuración del Filtrado de protocolos. Estas funciones son fundamentales para la protección del ordenador durante la comunicación a través de Internet.

La **Protección del cliente de correo electrónico** controla toda la comunicación por correo electrónico, protege el ordenador frente al código malicioso y le permite seleccionar la acción que se realizará al detectar una amenaza.

La **Protección del tráfico de Internet** supervisa la comunicación entre los navegadores web y los servidores remotos, y cumple las reglas HTTP y HTTPS. Esta función también le permite bloquear, permitir o excluir determinadas direcciones URL.

El **Filtrado de protocolos** es una función de protección avanzada para los protocolos de aplicaciones disponible en el motor de análisis ThreatSense. Este control es automático, independientemente de si se utiliza un navegador de Internet o un cliente de correo electrónico. También funciona para la comunicación cifrada (SSL/TLS).

NOTA: en Windows Server 2008 y Windows Server 2008 R2, la instalación del componente **Web y correo electrónico** está desactivada de forma predeterminada. Si desea instalar esta función, elija el tipo de instalación **Personalizada**. Si ya tiene <%PN%> instalado, puede ejecutar el programa de instalación de nuevo para modificar la instalación agregando el componente Web y correo electrónico.

5.4.1 Filtrado de protocolos

Filtrado de protocolos

El motor de análisis ThreatSense, que integra a la perfección todas las técnicas avanzadas de análisis de código malicioso, proporciona la protección antivirus para los protocolos de aplicación. El filtrado de protocolos funciona de manera automática, independientemente del navegador de Internet o el cliente de correo electrónico utilizados. Para editar la configuración cifrada (SSL), vaya a **Web y correo electrónico** > **SSL/TLS**.

Activar el control sobre el contenido del protocolo de la aplicación: se puede utilizar para desactivar el filtrado de protocolos. Tenga en cuenta que muchos componentes de ESET Mail Security (Protección del tráfico de Internet, Protección de protocolos de correo electrónico y Anti-Phishing) dependen de esto para funcionar.

Aplicaciones excluidas: le permite excluir determinadas direcciones remotas del filtrado de protocolos. Esta opción es útil cuando el filtrado de protocolos provoca problemas de compatibilidad.

Direcciones IP excluidas: le permite excluir determinadas aplicaciones del filtrado de protocolos. Esta opción es útil cuando el filtrado de protocolos provoca problemas de compatibilidad.

Clientes de correo electrónico y web: solo se utiliza en sistemas operativos Windows, y le permite seleccionar las

aplicaciones para las que se filtra todo el tráfico con el filtrado de protocolos, independientemente de los puertos utilizados.

Registrar la información necesaria para que el soporte técnico de ESET diagnostique los problemas de filtrado de protocolos: permite el registro avanzado de datos de diagnóstico y solo se debe utilizar cuando lo solicita el soporte técnico de ESET.

5.4.1.1 Aplicaciones excluidas

Para excluir del filtrado de contenido la comunicación de aplicaciones de red específicas, selecciónelas en la lista. No se comprobará la presencia de amenazas en la comunicación HTTP/POP3 de las aplicaciones seleccionadas. Se recomienda utilizar esta opción únicamente en aplicaciones que no funcionen correctamente cuando se comprueba su comunicación.

Las aplicaciones y los servicios que ya se hayan visto afectados por el filtrado de protocolos se mostrarán automáticamente al hacer clic en **Agregar**.

Editar: modifica las entradas seleccionadas de la lista.
Quitar: elimina las entradas seleccionadas de la lista.

5.4.1.2 Direcciones IP excluidas

Las direcciones IP de esta lista no se incluirán en el filtrado de contenidos del protocolo. No se comprobará la presencia de amenazas en las comunicaciones HTTP/POP3/IMAP entrantes y salientes de las direcciones seleccionadas. Esta opción se recomienda únicamente para direcciones que se sabe que son de confianza.

Agregar: haga clic para agregar una dirección IP, un intervalo de direcciones o una subred de un punto remoto al que se aplicará una regla.

Modificar: modifique las entradas seleccionadas de la lista.

Quitar: elimina las entradas seleccionadas de la lista.

5.4.1.3 Clientes de correo electrónico y web

NOTA: la arquitectura Plataforma de filtrado de Windows (WFP) se empezó a aplicar en Windows Vista Service Pack 1 y Windows Server 2008, y se utiliza para comprobar la comunicación de red. La sección **Clientes de correo electrónico y web** no se encuentra disponible porque la tecnología WFP utiliza técnicas de supervisión especiales.

Dada la ingente cantidad de código malicioso que circula en Internet, la navegación segura es un aspecto crucial para la protección de los ordenadores. Las vulnerabilidades de los navegadores web y los vínculos fraudulentos sirven de ayuda a este tipo de código para introducirse en el sistema de incógnito; por este motivo, ESET Mail Security se centra en la seguridad de los navegadores web. Cada aplicación que acceda a la red se puede marcar como un navegador de Internet. Las aplicaciones que ya utilicen protocolos para la comunicación o procedentes de las rutas seleccionadas se pueden añadir a la lista de clientes web y de correo electrónico.

5.4.2 SSL/TLS

ESET Mail Security puede buscar amenazas en las comunicaciones que utilizan el protocolo SSL/TLS. Puede utilizar varios modos de análisis para examinar las comunicaciones protegidas mediante el protocolo SSL: certificados de confianza, certificados desconocidos o certificados excluidos del análisis de comunicaciones protegidas mediante el protocolo SSL.

Activar el filtrado del protocolo SSL/TLS: si está desactivado el filtrado de protocolos, el programa no analizará las comunicaciones realizadas a través de SSL/TLS.

El **modo de filtrado del protocolo SSL/TLS** ofrece las opciones siguientes:

- **Modo automático**: seleccione esta opción para analizar todas las comunicaciones protegidas mediante el protocolo SSL/TLS, excepto las protegidas por certificados excluidos del análisis. Si se establece una comunicación nueva que utiliza un certificado firmado desconocido, no se le informará y la comunicación se filtrará automáticamente. Si accede a un servidor con un certificado que no sea de confianza pero que usted ha marcado como de confianza (se encuentra en la lista de certificados de confianza), se permite la comunicación con el servidor y se filtra el contenido del canal de comunicación.
- **Modo interactivo**: si introduce un sitio nuevo protegido mediante SSL/TLS (con un certificado desconocido), se muestra un cuadro de diálogo con las acciones posibles. Este modo le permite crear una lista de certificados SSL/TLS que se excluirán del análisis.

Bloquear la comunicación cifrada utilizando el protocolo obsoleto SSL v2: la comunicación establecida con la versión anterior del protocolo SSL se bloqueará automáticamente.

Certificado raíz

Certificado raíz: para que la comunicación SSL/TLS funcione correctamente en los navegadores y clientes de correo electrónico, es fundamental que el certificado raíz de ESET se agregue a la lista de certificados raíz conocidos (editores). **Agregar el certificado raíz a los navegadores conocidos** debe estar activada. Seleccione esta opción para agregar el certificado raíz de ESET a los navegadores conocidos (por ejemplo, Opera y Firefox) de forma automática. En los navegadores que utilicen el almacén de certificados del sistema, el certificado se agregará automáticamente (por ejemplo, en Internet Explorer).

Para aplicar el certificado en navegadores no admitidos, haga clic en **Ver certificado** > **Detalles** > **Copiar en archivo** y, a continuación, impórtelo manualmente en el navegador.

Validez del certificado

Si el certificado no se puede verificar mediante el almacén de TRCA: a veces no es posible verificar el certificado de un sitio web con el almacén de autoridades certificadoras de confianza (TRCA). Esto significa que el certificado ha sido firmado por algún usuario (por ejemplo, el administrador de un servidor web o una pequeña empresa) y que el hecho de confiar en él no siempre representa un riesgo. La mayoría de las empresas grandes (como los bancos) utilizan certificados firmados por TRCA. Si se ha seleccionado **Preguntar sobre la validez del certificado** (predeterminada), se le pedirá al usuario que seleccione la acción que desea realizar cuando se establezca la comunicación cifrada. Puede seleccionar **Bloquear las comunicaciones que usan el certificado** para finalizar siempre las conexiones cifradas a sitios que tienen certificados sin verificar.

Si el certificado no es válido o está dañado, significa que ha expirado o que la firma no es correcta. En este caso, se recomienda dejar seleccionada la opción **Bloquear las comunicaciones que usan el certificado**.

Lista de certificados conocidos le permite personalizar el comportamiento de ESET Mail Security con certificados SSL concretos.

5.4.2.1 Comunicación SSL cifrada

Si su sistema está configurado para utilizar el análisis del protocolo SSL, se mostrará un cuadro de diálogo para solicitarle que seleccione una acción en dos situaciones diferentes:

En primer lugar, si un sitio web utiliza un certificado no válido o que no se puede verificar y ESET Mail Security está configurado para preguntar al usuario en estos casos (la opción predeterminada es sí para los certificados que no se pueden verificar y no para los que no son válidos), se abre un cuadro de diálogo para preguntarle si desea **Permitir** o **Bloquear** la conexión.

En segundo lugar, si el **Modo de filtrado del protocolo SSL** está establecido en **Modo interactivo**, se mostrará un cuadro de diálogo para cada sitio web para preguntarle si desea **Analizar** o **Ignorar** el tráfico. Algunas aplicaciones comprueban que nadie haya modificado ni inspeccionado su tráfico SSL en estos casos, ESET Mail Security debe **Ignorar** el tráfico para que la aplicación siga funcionando.

En ambos casos, el usuario tiene la opción de recordar la acción seleccionada. Las acciones guardadas se almacenan en la **Lista de certificados conocidos**.

5.4.2.2 Lista de certificados conocidos

La lista de certificados conocidos se puede utilizar para personalizar el comportamiento de ESET Mail Security para determinados certificados SSL, así como para recordar las acciones elegidas al seleccionar el modo interactivo para el filtrado del protocolo SSL. La lista se puede ver y modificar en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Verificación del protocolo SSL** > **Lista de certificados conocidos**.

La ventana **Lista de certificados conocidos** consta de estos elementos:

Columnas

- **Nombre**: nombre del certificado.
- **Emisor del certificado**: nombre del creador del certificado.
- **Sujeto del certificado**: en este campo se identifica a la entidad asociada a la clave pública almacenada en el campo de clave pública del asunto.
- **Acceso**: seleccione **Permitir** o **Bloquear** como **Acción del acceso** para permitir o bloquear la comunicación que protege este certificado, independientemente de su fiabilidad. Seleccione **Auto** para permitir los certificados de confianza y preguntar cuando uno no sea de confianza. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.
- **Análisis**: seleccione **Análisis** o **Ignorar** como **Acción de análisis** para analizar o ignorar la comunicación que protege este certificado. Seleccione **Auto** para que el sistema realice el análisis en el modo automático y pregunte en el modo interactivo. Seleccione **Preguntar** para que el sistema siempre pregunte al usuario qué debe hacer.

Elementos de control

- **Editar**: seleccione el certificado que desea configurar y haga clic en **Editar**.
- **Quitar**: seleccione el certificado que desea eliminar y haga clic en **Quitar**.
- **Aceptar/Cancelar**: haga clic en **Aceptar** para guardar los cambios o en **Cancelar** para salir sin guardarlos.

5.4.3 Protección del cliente de correo electrónico

La integración de ESET Mail Security con clientes de correo electrónico aumenta el nivel de protección activa frente a código malicioso en los mensajes de correo electrónico. Si su cliente de correo electrónico es compatible, la integración se puede activar en ESET Mail Security. Al activar la integración, la barra de herramientas de ESET Mail Security se inserta directamente en el cliente de correo electrónico (la barra de herramientas de las versiones más recientes de Windows Live Mail no se inserta), aumentando así la eficacia de la protección de correo electrónico. Las opciones de integración están disponibles en **Configuración** > **Configuración avanzada** > **Web y correo electrónico** > **Protección del cliente de correo electrónico** > **Clientes de correo electrónico**.

Integración en el cliente de correo electrónico

Actualmente se admiten los siguientes clientes de correo electrónico: Microsoft Outlook, Outlook Express, Windows Mail y Windows Live Mail. La protección de correo electrónico funciona como un complemento para estos programas. La principal ventaja del complemento es el hecho de que es independiente del protocolo utilizado. Cuando el cliente de correo electrónico recibe un mensaje cifrado, este se descifra y se envía para el análisis de virus. Para ver una lista de clientes de correo electrónico compatibles y sus versiones, consulte el siguiente artículo de la base de conocimientos de ESET.

Aunque la integración no esté activada, la comunicación por correo electrónico sigue estando protegida por el módulo de protección del cliente de correo electrónico (POP3, IMAP).

Active **Deshabilitar la verificación en caso de cambios en el contenido del buzón de entrada** si el sistema se ralentiza cuando trabaja con su cliente de correo electrónico (solo MS Outlook). Esto puede suceder cuando recupera correo electrónico de Kerio Outlook Connector Store.

Correo electrónico que se analizará

Correo recibido: activa el análisis de los mensajes recibidos.
Correo enviado: activa el análisis de los mensajes enviados.
Correo leído: activa el análisis de los mensajes leídos.

Acción que se realizará en correos electrónicos infectados

Sin acciones: si esta opción está activada, el programa identificará los archivos adjuntos infectados, pero dejará los mensajes sin realizar ninguna acción.
Eliminar mensajes: el programa informará al usuario sobre las amenazas y eliminará el mensaje.
Mover el correo electrónico a la carpeta de elementos eliminados: los mensajes infectados se moverán automáticamente a la carpeta Elementos eliminados.
Mover mensajes a la carpeta: los mensajes infectados se moverán automáticamente a la carpeta especificada.

Carpeta: especifique la carpeta personalizada a la que desea mover el correo infectado que se detecte.

Repetir el análisis tras la actualización: activa el nuevo análisis tras una actualización de la base de firmas de virus.

Aceptar los resultados de los análisis realizados por otros módulos: al seleccionar esta opción, el módulo de protección de correo electrónico acepta los resultados del análisis de otros módulos de protección (análisis de los protocolos POP3 e IMAP).

5.4.3.1 Protocolos de correo electrónico

Los protocolos IMAP y POP3 son los más utilizados para recibir comunicaciones por correo electrónico en una aplicación de cliente de correo. ESET Mail Security proporciona protección para estos protocolos, independientemente del cliente de correo electrónico utilizado, y sin necesidad de volver a configurar el cliente de correo electrónico.

La verificación de los protocolos IMAP/IMAPS y POP3/POP3S se puede configurar en Configuración avanzada. Para acceder a esta configuración, despliegue **Web y correo electrónico** > **Protección del cliente de correo electrónico** > **Protocolos de correo electrónico**.

ESET Mail Security también admite el análisis de los protocolos IMAPS y POP3S, que utilizan un canal cifrado para

transferir información entre el servidor y el cliente. ESET Mail Security comprueba la comunicación con los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El programa solo analizará el tráfico de los puertos definidos en Puertos utilizados por el protocolo IMAPS/POP3S, independientemente de la versión del sistema operativo.

Las comunicaciones cifradas no se analizarán cuando se utilice la configuración predeterminada. Para activar el análisis de la comunicación cifrada, vaya a Verificación del protocolo SSL en Configuración avanzada, haga clic en **Web y correo electrónico** > **SSL/TLS** y seleccione **Activar el filtrado del protocolo SSL/TLS**.

5.4.3.2 Alertas y notificaciones

La protección del correo electrónico proporciona control de las comunicaciones por correo electrónico recibidas a través de los protocolos POP3 e IMAP. Con el complemento para Microsoft Outlook y otros clientes de correo electrónico, ESET Mail Security ofrece control de todas las comunicaciones desde el cliente de correo electrónico (POP3, MAPI, IMAP, HTTP). Al examinar los mensajes entrantes, el programa utiliza todos los métodos de análisis avanzados incluidos en el motor de análisis ThreatSense. Esto significa que la detección de programas maliciosos tiene lugar incluso antes de que se compare con la base de firmas de virus. El análisis de las comunicaciones de los protocolos POP3 e IMAP es independiente del cliente de correo electrónico utilizado.

Las opciones de esta función están disponibles en **Configuración avanzada**, en **Web y correo electrónico** > **Protección del cliente de correo electrónico** > **Alertas y notificaciones**.

Parámetros de ThreatSense: la configuración avanzada del análisis de virus le permite configurar objetos de análisis, métodos de detección, etc. Haga clic aquí para ver la ventana de configuración detallada del análisis de virus.

Después de analizar un mensaje de correo electrónico, se puede adjuntar al mensaje una notificación del análisis. Puede elegir entre las opciones **Notificar en los mensajes recibidos y leídos, Agregar una nota al asunto de los correos electrónicos infectados que fueron recibidos y leídos** o **Notificar en los mensajes enviados**. Tenga en cuenta que, en ocasiones puntuales, es posible que los mensajes con etiqueta se omitan en mensajes HTML problemáticos o que hayan sido falsificados por código malicioso. Los mensajes con etiqueta se pueden agregar a los mensajes recibidos y leídos, a los mensajes enviados o a ambos. Las opciones disponibles son:

- **Nunca**: no se agregará ningún mensaje con etiqueta.
- **Solo a mensajes infectados**: únicamente se marcarán como analizados los mensajes que contengan software malicioso (opción predeterminada).
- **A todos los mensajes analizados**: el programa agregará un mensaje a todo el correo analizado.

Agregar una nota al asunto de los correos electrónicos infectados enviados: desactive esta casilla de verificación si no desea que la protección de correo electrónico incluya una alerta de virus en el asunto de los mensajes infectados. Esta función permite el filtrado sencillo y por asunto de los mensajes infectados (si su programa de correo electrónico lo admite). Además, aumenta la credibilidad ante el destinatario y, si se detecta una amenaza, proporciona información valiosa sobre el nivel de amenaza de un correo electrónico o remitente determinado.

En mensajes infectados, agregar en el Asunto la siguiente etiqueta: modifique esta plantilla si desea modificar el formato de prefijo del asunto de un mensaje infectado. Esta función sustituye el asunto del mensaje *"Hello"* con un valor de prefijo especificado *"[virus]"* por el formato siguiente: *"[virus] Hello"*. La variable *%VIRUSNAME%* hace referencia a la amenaza detectada.

5.4.3.3 Barra de herramientas de MS Outlook

La protección de Microsoft Outlook funciona como un módulo de complemento. Una vez que se ha instalado ESET Mail Security, se añade a Microsoft Outlook esta barra de herramientas, que contiene las opciones del módulo de protección antivirus:

ESET Mail Security: al hacer clic en el icono se abre la ventana principal del programa de ESET Mail Security.

Analizar de nuevo los mensajes: le permite iniciar la comprobación del correo electrónico de forma manual. Puede especificar los mensajes que se comprobarán y activar un nuevo análisis del correo recibido. Para obtener más información, consulte Protección del cliente de correo electrónico.

Configuración del análisis: muestra las opciones de configuración de la Protección del cliente de correo electrónico.

5.4.3.4 Barra de herramientas de Outlook Express y Windows Mail

La protección para Outlook Express y Windows Mail funciona como un módulo de complemento. Una vez que se ha instalado ESET Mail Security, se añade a Outlook Express o Windows Mail esta barra de herramientas, que contiene las opciones del módulo de protección antivirus:

ESET Mail Security: al hacer clic en el icono se abre la ventana principal del programa de ESET Mail Security.

Analizar de nuevo los mensajes: le permite iniciar la comprobación del correo electrónico de forma manual. Puede especificar los mensajes que se comprobarán y activar un nuevo análisis del correo recibido. Para obtener más información, consulte Protección del cliente de correo electrónico.

Configuración del análisis: muestra las opciones de configuración de la Protección del cliente de correo electrónico.

Interfaz de usuario

Personalizar la apariencia: la apariencia de la barra de herramientas se puede modificar para el cliente de correo electrónico. Desactive la opción que personaliza la apariencia independientemente de los parámetros del programa de correo electrónico.

Mostrar texto: muestra descripciones de los iconos.

Texto a la derecha: las descripciones se mueven de la parte inferior al lado derecho de los iconos.

Iconos grandes: muestra iconos grandes para las opciones de menú.

5.4.3.5 Cuadro de diálogo de confirmación

Esta notificación sirve para comprobar que el usuario realmente desea realizar la acción seleccionada, que debería eliminar los posibles errores.

Por otra parte, el cuadro de diálogo también ofrece la posibilidad de desactivar las confirmaciones.

5.4.3.6 Analizar de nuevo los mensajes

La barra de herramientas de ESET Mail Security integrada en los clientes de correo electrónico permite a los usuarios especificar varias opciones de análisis del correo electrónico. La opción **Analizar de nuevo los mensajes** ofrece dos modos de análisis:

Todos los mensajes de la carpeta actual: analiza los mensajes de la carpeta que se muestra en ese momento.

Solo los mensajes seleccionados: analiza únicamente los mensajes marcados por el usuario.

La casilla de verificación **Volver a analizar los mensajes ya analizados** ofrece la posibilidad de ejecutar otro análisis en mensajes ya analizados.

5.4.4 Protección del tráfico de Internet

La conectividad de Internet es una característica estándar de la mayoría de los ordenadores personales. Lamentablemente también se ha convertido en el principal medio de transferencia de código malicioso, La protección del tráfico de Internet funciona supervisando la comunicación entre navegadores web y servidores remotos, y cumple con las reglas HTTP (Protocolo de transferencia de hipertexto) y HTTPS (comunicación cifrada).

El acceso a las páginas web que se sabe que contienen código malicioso se bloquea antes de descargar contenido. El motor de análisis ThreatSense analiza todas las demás páginas web cuando se cargan y bloquean en caso de detección de contenido malicioso. La protección del tráfico de Internet ofrece dos niveles de protección: bloqueo por lista negra y bloqueo por contenido.

Le recomendamos encarecidamente que deje activada la opción de protección del tráfico de Internet. A esta opción se puede acceder desde la ventana principal del programa de ESET Mail Security, en **Configuración** > **Ordenador** > **Protección del acceso a la Web**.

Las opciones siguientes están disponibles en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Protección del tráfico de Internet**:

- **Básico**: le permite activar o desactivar toda la Protección del acceso a la Web. Cuando esté desactivada, las opciones indicadas a continuación estarán inactivas.
- **Protocolos web**: le permite configurar la supervisión de estos protocolos estándar que utilizan la mayoría de los navegadores de Internet.
- **Gestión de direcciones URL**: aquí puede especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis.
- **Configuración de parámetros del motor ThreatSense**: la configuración avanzada del análisis de virus le permite configurar opciones como los tipos de objetos que desea analizar (mensajes de correo electrónico, archivos comprimidos, etc.), los métodos de detección para la protección del tráfico de Internet, etc.

Protocolos web

De forma predeterminada, ESET Mail Security está configurado para supervisar el protocolo HTTP que utilizan la mayoría de los navegadores de Internet.

En Windows Vista y versiones posteriores, el tráfico HTTP se supervisa siempre en todos los puertos y para todas las aplicaciones. En Windows XP/2003, se pueden modificar los puertos que utiliza el protocolo HTTP en **Configuración avanzada** (F5) > **Web y correo electrónico** > **Protección del tráfico de Internet** > **Protocolos web** > **Configuración del análisis HTTP**. El tráfico HTTP se supervisa en los puertos especificados para todas las aplicaciones, y en todos los puertos de las aplicaciones marcadas como Clientes de correo electrónico y web.

ESET Mail Security admite también la comprobación del protocolo HTTPS. La comunicación HTTPS utiliza un canal cifrado para transferir información entre el servidor y el cliente. ESET Mail Security comprueba la comunicación mediante los protocolos SSL (capa de sockets seguros) y TLS (seguridad de la capa de transporte). El programa solo analizará el tráfico de los puertos definidos en Puertos utilizados por el protocolo HTTPS, independientemente de la versión del sistema operativo.

La comunicación cifrada no se analizará cuando se utilice la configuración predeterminada. Para activar el análisis de la comunicación cifrada, vaya a Verificación del protocolo SSL en Configuración avanzada, haga clic en **Web y correo electrónico** > **Verificación del protocolo SSL** y seleccione **Activar el filtrado del protocolo SSL**.

5.4.4.1 Básico

Elija si desea tener la **Protección del acceso a la Web** activada (predeterminado) o desactivada. Cuando esté desactivada, las opciones indicadas a continuación estarán inactivas.

NOTA: le recomendamos encarecidamente que deje activada la opción Protección del acceso a la Web. A esta opción también se puede acceder desde la ventana principal del programa de ESET Mail Security, en **Configuración** > **Ordenador** > **Protección del acceso a la Web**.

5.4.4.2 Gestión de direcciones URL

En esta sección puede especificar las direcciones HTTP que desea bloquear, permitir o excluir del análisis.

No podrá acceder a los sitios web de Lista de direcciones bloqueadas, a menos que también se incluyan en Lista de direcciones permitidas. Cuando acceda a sitios web que se encuentran en Lista de direcciones que no se analizarán, no se buscará código malicioso en ellos.

Debe seleccionar Activar el filtrado del protocolo SSL/TLS si desea filtrar las direcciones HTTPS, además de las páginas web HTTP. Si no lo hace, solo se agregarán los dominios de los sitios HTTP que haya visitado, pero no la URL completa.

En todas las listas pueden utilizarse los símbolos especiales * (asterisco) y ? (signo de interrogación). El asterisco sustituye a cualquier número o carácter y el signo de interrogación, a cualquier carácter. Tenga especial cuidado al especificar direcciones excluidas, ya que la lista solo debe contener direcciones seguras y de confianza. Del mismo modo, es necesario asegurarse de que los símbolos * y ? se utilizan correctamente en esta lista.

Si desea bloquear todas las direcciones HTTP menos las incluidas en la **Lista de direcciones permitidas** activa, agregue el símbolo * a la **Lista de direcciones bloqueadas** activa.

Agregar: crea una lista nueva, que se suma a las predefinidas. Esta opción puede ser útil si se desea dividir varios grupos de direcciones de forma lógica. Por ejemplo, una lista de direcciones bloqueadas puede contener direcciones de algunas listas negras públicas externas, mientras que otra contiene su propia lista negra. Esto facilita la actualización de la lista externa sin que la suya se vea afectada.
Editar: modifica las listas existentes. Utilice esta opción para agregar o quitar direcciones en las listas.
Quitar: elimina la lista existente. Esta opción solo se puede usar en listas creadas con Agregar, no en las predeterminadas.

5.4.4.2.1 Crear nueva lista

En esta sección podrá indicar las listas de máscaras o direcciones URL que desea bloquear, permitir o excluir del análisis.

Cuando se crea una lista nueva, se pueden configurar las siguientes opciones:

Tipo de lista de direcciones: están disponibles tres tipos de listas:

- **Lista de direcciones que no se analizarán**: no se comprobará la existencia de código malicioso en ninguna de las direcciones agregadas a esta lista.
- **Lista de direcciones bloqueadas**: el usuario no tendrá acceso a las direcciones incluidas en esta lista. Esto se aplica exclusivamente al protocolo HTTP, no se bloquearán los protocolos que no sean HTTP.
- **Lista de direcciones permitidas**: si está activada la opción Permitir el acceso solo a las direcciones HTTP de la lista de direcciones permitidas y la lista de direcciones bloqueadas contiene un * (coincidir con todo), el usuario podrá acceder únicamente a las direcciones especificadas en esta lista. Las direcciones de esta lista estarán autorizadas incluso si se encuentran en la lista de direcciones bloqueadas.

Nombre de la lista: especifique el nombre de la lista. Este campo está desactivado cuando se edita una de las tres listas predefinidas.

Descripción de la lista: escriba una breve descripción de la lista (opcional). Este campo está desactivado cuando se edita una de las tres listas predefinidas.

Para activar una lista, seleccione **Lista activa** junto a ella. Si desea recibir una notificación cuando se utilice una lista determinada al evaluar un sitio HTTP que ha visitado, seleccione **Notificar cuando se aplique**. Por ejemplo, se emitirá una notificación si un sitio web se bloquea o admite porque se ha incluido en la lista de direcciones bloqueadas o permitidas. La notificación contendrá el nombre de la lista donde se incluye el sitio web especificado.

Agregar: agregar a la lista una dirección URL nueva (introduzca varios valores con un separador).

Editar: permite modificar la dirección existente en la lista. Solo se puede utilizar con direcciones que se hayan creado con la opción Agregar.

Quitar: elimina las direcciones existentes de la lista. Solo se puede utilizar con direcciones que se hayan creado con la opción Agregar.

Importar: permite importar un archivo con direcciones URL separadas por un salto de línea (por ejemplo, un archivo *.txt con codificación UTF-8).

5.4.4.2.2 Direcciones HTTP

En esta sección podrá indicar las listas de direcciones HTTP que desea bloquear, permitir o excluir del análisis.

De forma predeterminada, están disponibles estas tres listas:

- **Lista de direcciones que no se analizarán**: no se comprobará la existencia de código malicioso en ninguna de las direcciones agregadas a esta lista.
- **Lista de direcciones permitidas**: si está activada la opción **Permitir el acceso solo a las direcciones HTTP de la lista de direcciones permitidas** y la lista de direcciones bloqueadas contiene un * (coincidir con todo), el usuario podrá acceder únicamente a las direcciones especificadas en esta lista. Las direcciones de esta lista estarán autorizadas incluso si se incluyen en la lista de direcciones bloqueadas.
- **Lista de direcciones bloqueadas**: el usuario no tendrá acceso a las direcciones incluidas en esta lista a menos que aparezcan también en la lista de direcciones permitidas.

Haga clic en **Agregar** para crear una lista nueva. Para eliminar las listas seleccionadas, haga clic en **Quitar**.

5.4.5 Protección Anti-Phishing

<%PN%> también ofrece protección contra el phishing. La protección Anti-Phishing está integrada en el módulo Web y correo electrónico. Si ha instalado <%PN%> utilizando el tipo de instalación **Completa**, Web y correo electrónico se instala con la protección Anti-Phishing activada de forma predeterminada. No obstante, no se aplica a los sistemas en los que se ejecuta Microsoft Windows Server 2008.

NOTA: el componente Web y correo electrónico no se incluye en el tipo de instalación **Completa** <%PN%> en Windows Server 2008 o Windows Server 2008 R2. Si es necesario, puede modificar la instalación agregando el componente Web y correo electrónico para poder usar la protección Anti-Phishing.

El término phishing, o suplantación de la identidad, define una actividad delictiva que usa técnicas de ingeniería social (manipulación de los usuarios para obtener información confidencial). Su objetivo suele ser acceder a datos confidenciales como, por ejemplo, números de cuentas bancarias, códigos PIN, etc. Puede obtener más información sobre esta actividad en el glosario. ESET Mail Security incluye protección frente al phishing que bloquea páginas web conocidas por distribuir este tipo de contenido.

Recomendamos encarecidamente que active la protección Anti-Phishing en ESET Mail Security. Para ello, abra **Configuración avanzada** (F5) y acceda a **Web y correo electrónico** > **Protección Anti-Phishing**.

Visite este artículo de nuestra base de conocimiento para obtener más información sobre la protección Anti-Phishing de ESET Mail Security.

Acceso a un sitio web de phishing

Cuando entre en un sitio web de phishing reconocido se mostrará el siguiente cuadro de diálogo en su navegador web. Si aún así quiere acceder al sitio web, haga clic en **Ir al sitio** (no recomendado).

Alerta: ESET Mail Security
ESET MAIL SECURITY
Posible intento de phishing
Esta página se ha identificado como página objeto de phishing. Mostrar URL
Las páginas objeto de phishing suelen tener un aspecto similar a las páginas de bancos conocidos o instituciones de confianza y su objetivo es obtener información personal como nombres de usuario, contraseñas o datos de tarjetas de crédito. No se recomienda el acceso a esta páginas.
Obtener más información acerca del phishing
Esta página no es objeto de phishing
Volver
Ir al sitio
Abrir base de conocimientos de ESET | www.eset.es

NOTA: los posibles sitios de phishing que se han incluido en la lista blanca expirarán de forma predeterminada después de unas horas. Para permitir un sitio web permanentemente, use la herramienta Gestión de direcciones

URL. En **Configuración avanzada** (F5), despliegue **Web y correo electrónico** > **Protección del tráfico de Internet** > **Gestión de direcciones URL**> **Lista de direcciones**, haga clic en **Editar** y agregue a la lista el sitio web que desee modificar.

Cómo informar de sitios de phishing

El enlace Informar le permite informar de un sitio web de phishing o malicioso para que ESET lo analice.

NOTA: antes de enviar un sitio web a ESET, asegúrese de que cumple uno o más de los siguientes criterios:

- El sitio web no se detecta en absoluto.
- El sitio web se detecta como una amenaza, pero no lo es. En este caso, puede informar de un falso positivo de phishing.

También puede enviar el sitio web por correo electrónico. Envíe su correo electrónico a samples@eset.com. Utilice un asunto descriptivo y adjunte toda la información posible sobre el sitio web (por ejemplo, el sitio web que le refirió a este, cómo tuvo constancia de su existencia, etc.).

5.5 Control de dispositivos

ESET Mail Security permite controlar los dispositivos automáticamente (CD, DVD, USB, etc.). Este módulo le permite analizar, bloquear o ajustar los filtros y permisos ampliados, así como establecer los permisos de un usuario para acceder a un dispositivo dado y trabajar en él. Esto puede ser útil cuando el administrador del ordenador quiere impedir que los usuarios utilicen dispositivos con contenido no solicitado.

Dispositivos externos admitidos:

- Almacenamiento en disco (unidad de disco duro, disco USB extraíble)
- CD/DVD
- Impresora USB
- Almacenamiento FireWire
- Dispositivo Bluetooth
- Lector de tarjetas inteligentes
- Dispositivo de imagen
- Módem
- Puerto LPT/COM
- Dispositivo portátil
- Todos los tipos de dispositivos

Las opciones de configuración del control de dispositivos se pueden modificar en **Configuración avanzada** (F5) > **Control de dispositivos**.

Al activar el conmutador situado junto a **Integrar en el sistema** se activa la característica de control de dispositivos en ESET Mail Security; deberá reiniciar el ordenador para que se aplique este cambio. Una vez que el control de dispositivos esté activado, se activará el **Editor de reglas**, lo que le permitirá abrir la ventana Editor de reglas.

Si se inserta un dispositivo que está bloqueado por una regla, se muestra una ventana de notificación y se prohíbe el acceso a dicho dispositivo.

5.5.1 Reglas de control de dispositivos

La ventana **Editor de reglas de control de dispositivos** muestra las reglas existentes para dispositivos externos que los usuarios conectan al ordenador y permite controlarlos de forma precisa.

Determinados dispositivos se pueden permitir o bloquear por usuario, por grupo de usuarios o según varios parámetros adicionales que se pueden especificar en la configuración de las reglas. La lista de reglas contiene varias descripciones de una regla, como el nombre, el tipo de dispositivo externo, la acción que debe realizarse tras conectar un dispositivo externo al ordenador y la gravedad del registro.

Haga clic en **Agregar** o en **Modificar** para administrar una regla. Haga clic en **Quitar** si desea eliminar la regla seleccionada o anule la selección de la casilla de verificación **Activado** junto a una regla dada para desactivarla. Esta

opción puede ser útil si no desea eliminar una regla de forma permanente para poder utilizarla más adelante.

Copiar: crea una regla nueva basada en los parámetros de la regla seleccionada.

Haga clic en **Llenar** para rellenar automáticamente los parámetros del medio extraíble conectado a su ordenador.

Las reglas se muestran en orden de prioridad; las que tienen más prioridad se muestran más arriba en la lista. Puede seleccionar varias reglas y aplicar acciones —como eliminarlas o moverlas en la lista con los botones **Superior/ Arriba/Abajo/Inferior**— (botones de flecha).

Las entradas de registro se pueden ver desde la ventana principal del programa de ESET Mail Security en **Herramientas** > Archivos de registro.

5.5.2 Adición de reglas de control de dispositivos

Una regla de control de dispositivos define la acción que se realizará al conectar al ordenador un dispositivo que cumple los criterios de la regla.

Introduzca una descripción de la regla en el campo **Nombre** para facilitar la identificación. Haga clic en el conmutador situado junto a **Regla activada** para activar o desactivar esta regla, lo cual puede ser de utilidad cuando no se quiere eliminar una regla de forma permanente.

Tipo de dispositivo

Elija el tipo de dispositivo externo en el menú desplegable (Almacenamiento en disco, Dispositivo portátil, Bluetooth, FireWire…). Los tipos de dispositivos se heredan del sistema operativo y se pueden ver en el administrador de dispositivos del sistema cada vez que se conecta un dispositivo al ordenador. Los dispositivos de almacenamiento abarcan discos externos o lectores de tarjetas de memoria convencionales conectados mediante USB o FireWire. Los lectores de tarjetas inteligentes abarcan todos los lectores que tienen incrustado un circuito integrado, como las tarjetas SIM o las tarjetas de autenticación. Ejemplos de dispositivos de imagen son escáneres o cámaras; estos dispositivos no proporcionan información sobre los usuarios, sino únicamente sobre sus acciones. Esto significa que los dispositivos de imagen solo se pueden bloquear globalmente.

Acción

El acceso a dispositivos que no son de almacenamiento se puede permitir o bloquear. En cambio, las reglas para los dispositivos de almacenamiento permiten seleccionar una de las siguientes configuraciones de derechos:

- **Lectura/Escritura**: se permitirá el acceso completo al dispositivo.
- **Bloquear**: se bloqueará el acceso al dispositivo.
- **Solo lectura**: solo se permitirá el acceso de lectura al dispositivo.
- **Advertir**: cada vez que se conecte un dispositivo se informará al usuario de si está permitido o bloqueado, y se efectuará una entrada de registro. Los dispositivos no se recuerdan, se seguirá mostrando una notificación en las siguientes conexiones del mismo dispositivo.

Tenga en cuenta que no todos los derechos (acciones) están disponibles para todos los tipos de dispositivos. Si un dispositivo dispone de espacio de almacenamiento, estarán disponibles las cuatro acciones. Para los dispositivos que no son de almacenamiento, solo hay solo dos (por ejemplo, **Solo lectura** no está disponible para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir o bloquear).

Debajo se muestran otros parámetros que se pueden usar para ajustar las reglas y adaptarlas a dispositivos. Todos los parámetros distinguen entre mayúsculas y minúsculas:

- **Fabricante**: filtrado por nombre o identificador del fabricante.
- **Modelo**: el nombre del dispositivo.
- **Número de serie**: normalmente, los dispositivos externos tienen su propio número de serie. En el caso de los CD y DVD, el número de serie está en el medio, no en la unidad de CD.

NOTA: si estas tres descripciones mencionadas están vacías, la regla ignorará estos campos al establecer la coincidencia. Los parámetros de filtrado de todos los campos de texto no distinguen entre mayúsculas y minúsculas, y no admiten caracteres comodín (*, ?).

Sugerencia: si desea averiguar los parámetros de un dispositivo, cree una regla para permitir ese tipo de dispositivo,

conecte el dispositivo al ordenador y, a continuación, consulte los detalles del dispositivo en el Registro de control de dispositivos.

Nivel de registro

- **Siempre**: registra todos los sucesos.
- **Diagnóstico**: registra la información necesaria para ajustar el programa.
- **Información**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alerta**: registra errores graves y mensajes de alerta.
- **Ninguno**: no se registra nada.

Las reglas se pueden limitar a determinados usuarios o grupos de usuarios agregándolos a la **Lista de usuarios**:

- **Agregar**: abre el cuadro de diálogo **Tipos de objeto: Usuarios o grupos**, que le permite seleccionar los usuarios que desee.
- **Quitar**: elimina del filtro al usuario seleccionado.

NOTA: los dispositivos se pueden filtrar mediante reglas de usuario (por ejemplo, los dispositivos de imagen no proporcionan información sobre los usuarios, sino únicamente sobre las acciones invocadas).

5.5.3 Dispositivos detectados

El botón **Llenar** contiene una visión general de todos los dispositivos conectados actualmente con la siguiente información: tipo de dispositivo, proveedor del dispositivo, modelo y número de serie (si está disponible). Cuando selecciona un dispositivo (de la lista de dispositivos detectados) y hace clic en **Aceptar**, aparece una ventana del editor de reglas con información predefinida (puede modificar todos los ajustes).

5.5.4 Grupos de dispositivos

La conexión de un dispositivo al ordenador puede presentar un riesgo para la seguridad.

La ventana Grupos de dispositivos se divide en dos partes. La parte derecha de la ventana contiene una lista de los dispositivos que pertenecen al grupo correspondiente, mientras que la parte izquierda contiene los grupos existentes. Seleccione el grupo que contiene los dispositivos que desea mostrar en el panel derecho.

Cuando abre la ventana Grupos de dispositivos y selecciona uno de los grupos, puede agregar o quitar dispositivos de la lista. Otra forma de agregar dispositivos al grupo es importarlos desde un archivo. También puede hacer clic en **Llenar** y se mostrarán en la ventana **Dispositivos detectados** todos aquellos dispositivos que estén conectados a su ordenador. Seleccione un dispositivo de la lista para agregarlo al grupo haciendo clic en **Aceptar**.

Elementos de control

Agregar: puede agregar un grupo al especificar su nombre, así como agregar un dispositivo a un grupo existente (si lo desea puede especificar detalles como el nombre del proveedor, el modelo y el número de serie), en función de la parte de la ventana en la que hiciera clic.

Editar: le permite modificar el nombre del grupo seleccionado o los parámetros (proveedor, modelo, número de serie) de los dispositivos que este contiene.

Quitar: elimina el grupo o el dispositivo seleccionados, según la parte de la ventana en la que hiciera clic.

Importar: importa una lista de dispositivos desde un archivo.

El botón **Llenar** contiene una visión general de todos los dispositivos conectados actualmente con la siguiente información: tipo de dispositivo, proveedor del dispositivo, modelo y número de serie (si está disponible).

Cuando haya finalizado la personalización, haga clic en **Aceptar**. Haga clic en **Cancelar** si desea cerrar la ventana **Grupos de dispositivos** sin guardar los cambios.

CONSEJO: puede crear varios grupos de dispositivos a los que se aplicarán reglas distintas. También puede crear solo un grupo de dispositivos al que se aplicará la regla con la acción **Lectura/Escritura** o **Solo lectura**. Esto garantiza el

bloqueo de dispositivos no reconocidos por el control de dispositivos pero conectados al ordenador.

Tenga en cuenta que no todas las acciones (permisos) están disponibles para todos los tipos de dispositivos. En los dispositivos de almacenamiento están disponibles las cuatro acciones. En el caso de los dispositivos que no son de almacenamiento solo hay tres disponibles (por ejemplo, **Solo lectura** no está disponible para Bluetooth, lo que significa que los dispositivos Bluetooth solo se pueden permitir, bloquear o emitirse una advertencia sobre ellos).

5.6 Herramientas

A continuación se exponen los ajustes avanzados de todas las herramientas que ESET Mail Security ofrece en la ficha **Herramientas** de la ventana de la interfaz gráfica de usuario principal.

5.6.1 ESET Live Grid

ESET Live Grid es un sistema avanzado de alerta temprana compuesto por varias tecnologías basadas en la nube. Ayuda a detectar las amenazas emergentes según su reputación, y mejora el rendimiento de análisis mediante la creación de listas blancas. La nueva información sobre la amenaza se transmite en tiempo real a la nube, lo que permite que el laboratorio de investigación de software malicioso de ESET responda a tiempo y mantenga una protección constante en todo momento. Los usuarios pueden consultar la reputación de los archivos y procesos en ejecución directamente en la interfaz del programa o en el menú contextual; además, disponen de información adicional en ESET Live Grid. Seleccione una de las siguientes opciones durante la instalación de ESET Mail Security:

1. La activación de ESET Live Grid no es obligatoria. El software no perderá funcionalidad, pero puede que ESET Mail Security responda más lento a las nuevas amenazas que la actualización de la base de firmas de virus.
2. Puede configurar ESET Live Grid para enviar información anónima acerca de nuevas amenazas y sobre la ubicación del nuevo código malicioso detectado. Este archivo se puede enviar a ESET para que realice un análisis detallado. El estudio de estas amenazas ayudará a ESET a actualizar sus funciones de detección de amenazas.

ESET Live Grid recopilará información anónima del ordenador relacionada con las amenazas detectadas recientemente. Esta información puede incluir una muestra o copia del archivo donde haya aparecido la amenaza, la ruta a ese archivo, el nombre de archivo, la fecha y la hora, el proceso por el que apareció la amenaza en el ordenador e información sobre el sistema operativo del ordenador.

De forma predeterminada, ESET Mail Security está configurado para enviar archivos sospechosos para su análisis detallado en el laboratorio de virus de ESET. Los archivos con determinadas extensiones, como *.doc* o *.xls*, se excluyen siempre. También puede agregar otras extensiones para excluir los archivos que usted o su empresa no deseen enviar.

El sistema de reputación de ESET Live Grid ofrece listas blancas y negras basadas en la nube. Si desea acceder a la configuración de ESET Live Grid, pulse F5 para ir a Configuración avanzada y expanda **Herramientas** > **ESET Live Grid**.

Activar el sistema de reputación ESET Live Grid (recomendado): el sistema de reputación ESET Live Grid mejora la eficiencia de las soluciones contra software malicioso de ESET mediante la comparación de los archivos analizados con una base de datos de elementos incluidos en listas blancas y negras disponibles en la nube.

Enviar estadísticas anónimas: permita a ESET recopilar información sobre nuevas amenazas detectadas, como el nombre de la amenaza, información sobre la fecha y hora en la que se detectó, el método de detección y los metadatos asociados y la versión y la configuración del producto la versión del producto, incluida información sobre su sistema.

Enviar archivos: los archivos sospechosos que por su comportamiento inusual o características recuerdan a amenazas se envían a ESET para su análisis.

Seleccione **Activar el registro de sucesos** para crear un registro de sucesos en el que anotar los envíos de archivos e información estadística. Permitirá agregar anotaciones al registro de sucesos cuando se envíen archivos o información estadística.

Correo electrónico de contacto (opcional): su correo electrónico de contacto se puede enviar con cualquier archivo sospechoso y puede servir para localizarle si se necesita más información para el análisis. Tenga en cuenta que no recibirá una respuesta de ESET, a no ser que sea necesaria más información.

Exclusiones: esta opción le permite excluir del envío determinados archivos o carpetas (por ejemplo, puede ser útil para excluir archivos que puedan contener información confidencial, como documentos u hojas de cálculo). Los archivos mostrados en la lista nunca se enviarán al laboratorio de ESET para su análisis, aunque contengan código sospechoso. Los tipos de archivos más comunes se excluyen de manera predeterminada (.doc, etc.). Si lo desea, puede añadir elementos a la lista de archivos excluidos.

Si utilizó ESET Live Grid anteriormente pero lo desactivó, es posible que aún haya paquetes de datos pendientes de envío. Estos paquetes se enviarán a ESET incluso después de la desactivación. Una vez que se haya enviado toda la información actual, no se crearán más paquetes.

5.6.1.1 Filtro de exclusión

La opción **Editar** disponible junto a Exclusiones en ESET Live Grid le permite configurar el modo de envío de las amenazas al laboratorio de virus de ESET para su análisis.

Si encuentra un archivo sospechoso, puede enviarlo a nuestros laboratorios para su análisis. Si resulta ser una aplicación maliciosa, su detección se agregará a la siguiente actualización de la base de firmas de virus.

5.6.2 Cuarentena

Los archivos infectados o sospechosos se almacenan, sin ningún tipo de impacto, en la carpeta de cuarentena. De manera predeterminada, el módulo de protección en tiempo real pone en cuarentena todos los archivos sospechosos creados recientemente con el fin de evitar infecciones.

Analizar nuevamente los archivos en Cuarentena después de cada actualización: después de cada actualización de la base de firmas de virus, se analizarán todos los objetos en cuarentena. Esto resulta especialmente útil si se ha movido un archivo a la cuarentena como consecuencia de la detección de un falso positivo. Si esta opción está activada, ciertos tipos de archivos se pueden restaurar automáticamente a su ubicación original.

5.6.3 Microsoft Windows Update

Las actualizaciones de Windows ofrecen correcciones importantes de vulnerabilidades potencialmente peligrosas, y mejoran el nivel de seguridad global del ordenador. Por este motivo, es fundamental que instale las actualizaciones de Microsoft Windows en cuanto se publiquen. ESET Mail Security le informa sobre las actualizaciones que le faltan, según el nivel que haya especificado. Están disponibles los siguientes niveles:

- **Sin actualizaciones**: no se ofrecerá ninguna actualización del sistema para la descarga.
- **Actualizaciones opcionales**: se ofrecerán para la descarga las actualizaciones marcadas como de baja prioridad y de niveles superiores.
- **Actualizaciones recomendadas**: se ofrecerán para la descarga las actualizaciones marcadas como habituales y de niveles superiores.
- **Actualizaciones importantes**: se ofrecerán para la descarga las actualizaciones marcadas como importantes y de niveles superiores.
- **Actualizaciones críticas**: solo se ofrecerá la descarga de actualizaciones críticas.

Haga clic en **Aceptar** para guardar los cambios. La ventana de actualizaciones del sistema se mostrará después de la verificación del estado con el servidor de actualización. Es posible que la información de actualización del sistema no esté disponible inmediatamente después de guardar los cambios.

5.6.4 Proveedor WMI

Acerca de WMI

El Instrumental de administración de Windows (WMI) es la implementación de Microsoft de WBEM (siglas del inglés Web-Based Enterprise Management), iniciativa que el sector ha adoptado para desarrollar una tecnología estándar a la hora de obtener acceso a la información de administración en entornos empresariales.

Si desea obtener más información sobre WMI, consulte http://msdn.microsoft.com/en-us/library/windows/desktop/aa384642(v=vs.85).aspx (en inglés).

Proveedor WMI de ESET

La finalidad del Proveedor WMI de ESET es permitir la supervisión remota de los productos de ESET en un entorno empresarial sin necesidad de software o herramientas propios de ESET. Al exponer la información básica del producto, su estado y estadísticas a través de WMI, crecen considerablemente las posibilidades que los administradores de las empresas tienen a su disposición durante la supervisión de los productos de ESET. Los administradores tendrán la posibilidad de emplear los diversos métodos de acceso ofrecidos por WMI (línea de comandos, scripts y herramientas de supervisión de terceros) para supervisar el estado de los productos de ESET.

En la implementación actual se permite acceso de solo lectura a información básica del producto, funciones instaladas y su estado de protección, estadísticas de módulos de análisis concretos y archivos de registro del producto.

El Proveedor WMI permite utilizar una infraestructura y herramientas estándar de Windows WMI para leer el estado y los registros del producto.

5.6.4.1 Datos proporcionados

Todas las clases WMI relacionadas con el producto ESET se encuentran en el espacio de nombres "root\ESET". A día de hoy están implementadas las siguientes clases, descritas a continuación con más detalle:

General:

- ESET_Product
- ESET_Features
- ESET_Statistics

Registros:

- ESET_ThreatLog
- ESET_EventLog
- ESET_ODFileScanLogs
- ESET_ODFileScanLogRecords
- ESET_ODServerScanLogs
- ESET_ODServerScanLogRecords
- ESET_GreylistLog
- ESET_SpamLog

ESET_Product class

Solo puede haber una instancia de la clase ESET_Product. Las propiedades de esta clase hacen referencia a información básica sobre el producto ESET instalado:

- **ID**: identificador de tipo del producto, por ejemplo "essbe".
- **Name**: nombre del producto, por ejemplo, "ESET Security".
- **Edition**: versión del producto, por ejemplo "Microsoft SharePoint Server".
- **Version**: versión del producto, por ejemplo "4.5.15013.0".
- **VirusDBVersion**: versión de la base de datos de virus, por ejemplo "7868 (20130107)".
- **VirusDBLastUpdate**: fecha y hora de la última actualización de la base de datos de virus. La cadena contiene la fecha y la hora en formato WMI, por ejemplo "20130118115511.000000+060".
- **LicenseExpiration**: plazo de caducidad de la licencia. La cadena contiene la fecha y la hora en formato WMI, por ejemplo "20130118115511.000000+060".
- **KernelRunning**: valor booleano que indica si el servicio eKrn se encuentra en ejecución en el ordenador, por ejemplo, "TRUE"
- **StatusCode**: número que indica el estado de protección del producto: 0: verde (correcto); 1: amarillo (advertencia); 2: rojo (error)
- **StatusText**: mensaje que describe el motivo de un código de estado que no sea cero; de lo contrario será un valor nulo.

ESET_Features class

La clase ESET_Features cuenta con varias instancias, en función del número de funciones del producto. Cada instancia contiene los siguientes elementos:

- **Name**: nombre de la función (a continuación se expone la lista de nombres).
- **Status**: estado de la función: 0: inactiva; 1: desactivada, 2; activada.

Una lista de cadenas que representa las funciones del producto actualmente reconocidas:

- **CLIENT_FILE_AV**: protección antivirus del sistema de archivos en tiempo real.
- **CLIENT_WEB_AV**: protección antivirus de Internet del cliente.
- **CLIENT_DOC_AV**: protección antivirus de documentos del cliente.
- **CLIENT_NET_FW**: cortafuegos personal del cliente.
- **CLIENT_EMAIL_AV**: protección antivirus del correo electrónico del cliente.
- **CLIENT_EMAIL_AS**: protección antispam del correo electrónico del cliente.
- **SERVER_FILE_AV**: protección antivirus en tiempo real de archivos del producto de servidor de archivos protegido; por ejemplo, archivos en la base de datos de contenido de SharePoint en el caso de ESET Mail Security.
- **SERVER_EMAIL_AV**: protección antivirus de correos electrónicos de producto de servidor protegido, por ejemplo correos electrónicos en MS Exchange o IBM Domino
- **SERVER_EMAIL_AS**: protección antispam de correos electrónicos de producto de servidor protegido, por ejemplo correos electrónicos en MS Exchange o IBM Domino
- **SERVER_GATEWAY_AV**: protección antivirus de protocolos de red protegidos en la puerta de enlace.
- **SERVER_GATEWAY_AS**: protección antispam de protocolos de red protegidos en la puerta de enlace.

ESET_Statistics class

La clase ESET_Statistics cuenta con varias instancias, en función del número de módulos de análisis del producto. Cada instancia contiene los siguientes elementos:

- Scanner: código de cadena del escáner concreto, por ejemplo "CLIENT_FILE".
- Total: número total de archivos analizados.
- Infected: número de archivos infectados detectados.
- Cleaned: número de archivos desinfectados.
- Timestamp: hora y fecha del último cambio de esta estadística. En formato de fecha y hora WMI, por ejemplo, "20130118115511.000000+060".
- ResetTime: fecha y hora del último restablecimiento del contador de estadísticas. En formato de fecha y hora WMI, por ejemplo, "20130118115511.000000+060".

Lista de cadenas que representan módulos de análisis actualmente reconocidos:

- CLIENT_FILE
- CLIENT_EMAIL
- CLIENT_WEB
- SERVER_FILE
- SERVER_EMAIL
- SERVER_WEB

ESET_ThreatLog class

La clase ESET_ThreatLog cuenta con varias instancias, y cada una de ellas representa un historial del registro "Detected threats". Cada instancia contiene los siguientes elementos:

- **ID**: identificador único de este historial del registro.
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI).
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Scanner**: nombre del módulo de análisis que creó este suceso del registro.
- **ObjectType**: tipo de objeto que generó este suceso del registro.
- **ObjectName**: nombre del objeto que generó este suceso del registro.
- **Threat**: nombre de la amenaza detectada en el objeto descrito por las propiedades ObjectName y ObjectType.
- **Action**: acción efectuada tras la identificación de la amenaza.
- **User**: cuenta de usuario que provocó la generación de este suceso del registro.
- **Information**: descripción adicional del evento.

ESET_EventLog

La clase ESET_EventLog cuenta con varias instancias, y cada una de ellas representa un historial del registro "Events". Cada instancia contiene los siguientes elementos:

- **ID**: identificador único de este historial del registro.
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI).
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Module**: nombre del módulo de análisis que creó este suceso del registro.
- **Event**: descripción del suceso.
- **User**: cuenta de usuario que provocó la generación de este suceso del registro.

ESET_ODFileScanLogs

La clase ESET_ODFileScanLogs cuenta con varias instancias, y cada una de ellas representa un registro de análisis de archivo a petición. Equivale a la lista de registros "On-demand computer scan" de la interfaz gráfica de usuario. Cada instancia contiene los siguientes elementos:

- **ID**: identificador único de este registro a petición.
- **Timestamp**: hora y fecha de creación del registro (en formato de fecha y hora WMI).
- **Targets**: carpetas/objetos destino del análisis.
- **TotalScanned**: número total de objetos analizados.
- **Infected**: número de objetos infectados encontrados.
- **Cleaned**: número de objetos desinfectados.
- **Status**: estado del proceso de análisis.

ESET_ODFileScanLogRecords

La clase ESET_ODFileScanLogRecords cuenta con varias instancias, y cada una de ellas representa un historial del registro en uno de los registros de análisis representados por las instancias de la clase ESET_ODFileScanLogs. Las instancias de esta clase contienen historiales de registro de todos los análisis/registros a petición. Cuando solo se requiere la instancia de un registro de análisis determinado, debe filtrarse por medio de la propiedad LogID. Cada instancia de la clase contiene los siguientes elementos:

- **LogID**: identificador del registro de análisis al que pertenece este historial (identificador de una de las instancias de la clase ESET_ODFileScanLogs).
- **ID**: identificador único de este historial del registro de análisis.
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI).
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log**: mensaje de registro real.

ESET_ODServerScanLogs

La clase ESET_ODServerScanLogs cuenta con varias instancias, y cada una de ellas representa una ejecución del análisis a petición del servidor. Cada instancia contiene los siguientes elementos:

- **ID**: identificador único de este registro a petición.
- **Timestamp**: hora y fecha de creación del registro (en formato de fecha y hora WMI).
- **Targets**: carpetas/objetos destino del análisis.
- **TotalScanned**: número total de objetos analizados.
- **Infected**: número de objetos infectados encontrados.
- **Cleaned**: número de objetos desinfectados.
- **RuleHits**: número total de coincidencias de la regla.
- **Status**: estado del proceso de análisis.

ESET_ODServerScanLogRecords

La clase ESET_ODServerScanLogRecords cuenta con varias instancias, y cada una de ellas representa un historial del registro en uno de los registros de análisis representados por las instancias de la clase ESET_ODServerScanLogRecords. Las instancias de esta clase contienen historiales de registro de todos los análisis/registros a petición. Cuando solo se requiere la instancia de un registro de análisis determinado, debe filtrarse por medio de la propiedad LogID. Cada instancia de la clase contiene los siguientes elementos:

- **LogID**: identificador del registro de análisis al que pertenece este historial (identificador de una de las instancias de la clase ESET_ODServerScanLogRecords).
- **ID**: identificador único de este historial del registro de análisis.
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI).
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Log**: mensaje de registro real.

ESET_GreylistLog

La clase ESET_GreylistLog cuenta con varias instancias, y cada una de ellas representa un historial del registro "Greylist". Cada instancia contiene los siguientes elementos:

- **ID**: identificador único de este historial del registro.
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI).
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **HELODomain**: nombre del dominio HELO.
- **IP**: dirección IP de origen.
- **Sender**: remitente del correo electrónico.
- **Recipient**: destinatario del correo electrónico.
- **Action**: acción realizada.
- **TimeToAccept**: cantidad de minutos tras la que se aceptará el correo electrónico.

ESET_SpamLog

La clase ESET_SpamLog cuenta con varias instancias, y cada una de ellas representa un historial del registro "Spamlog". Cada instancia contiene los siguientes elementos:

- **ID**: identificador único de este historial del registro.
- **Timestamp**: hora y fecha de creación del historial del registro (en formato de fecha y hora WMI).
- **LogLevel**: gravedad del historial del registro expresado como número en la escala [0-8]. Los valores corresponden a los siguientes niveles: Debug, Info-Footnote, Info, Info-Important, Warning, Error, SecurityWarning, Error-Critical, SecurityWarning-Critical
- **Sender**: remitente del correo electrónico.
- **Recipients**: destinatarios del correo electrónico.
- **Subject**: asunto del correo electrónico.
- **Received**: hora de recepción.
- **Score**: puntuación de spam expresada en porcentaje [0-100].
- **Reason**: motivo por el que este correo electrónico se marcó como correo no deseado.
- **Action**: acción realizada.
- **DiagInfo**: información de diagnóstico adicional.

5.6.4.2 Acceso a datos proporcionados

A continuación se exponen varios ejemplos de cómo acceder a los datos WMI de ESET desde la línea de comandos de Windows y PowerShell, herramientas que deberían funcionar en cualquier sistema operativo Windows. Además de estas, hay otras muchas formas de acceder a los datos desde otros lenguajes y herramientas de scripts.

Línea de comandos sin scripts

La herramienta de línea de comandos `wmic` puede utilizarse para acceder a varias clases WMI predefinidas y personalizadas.

Si desea mostrar información completa sobre el producto del ordenador local:
```
wmic /espacio de nombres:\\root\Ruta de acceso de ESET ESET_Product
```

Para mostrar únicamente el número de versión del producto del ordenador local:
```
wmic /espacio de nombres:\\root\Ruta de acceso de ESET ESET_Product Get Version
```

Para mostrar toda la información del producto de un ordenador remoto con la IP 10.1.118.180:
```
wmic /espacio de nombres:\\root\ESET /node:10.1.118.180 /user:Ruta del administrador ESET_Product
```

PowerShell

Obtener y mostrar información completa sobre el producto del ordenador local:
```
Get-WmiObject ESET_Product -espacionombres 'root\ESET'
```

Obtener y mostrar toda la información del producto de un ordenador remoto con la IP 10.1.118.180:
```
$cred = Get-Credential            # solicita al usuario credenciales y las almacena en la variable
Get-WmiObject ESET_Product -espacionombres 'root\ESET' -nombreordenador '10.1.118.180' -cred $cred
```

5.6.5 Objetos de análisis de ERA

Esta función permite que ESET Remote Administrator utilice objetos de análisis de base de datos a petición apropiados cuando se ejecuta la tarea **Análisis del servidor** cliente en un servidor con ESET Mail Security.

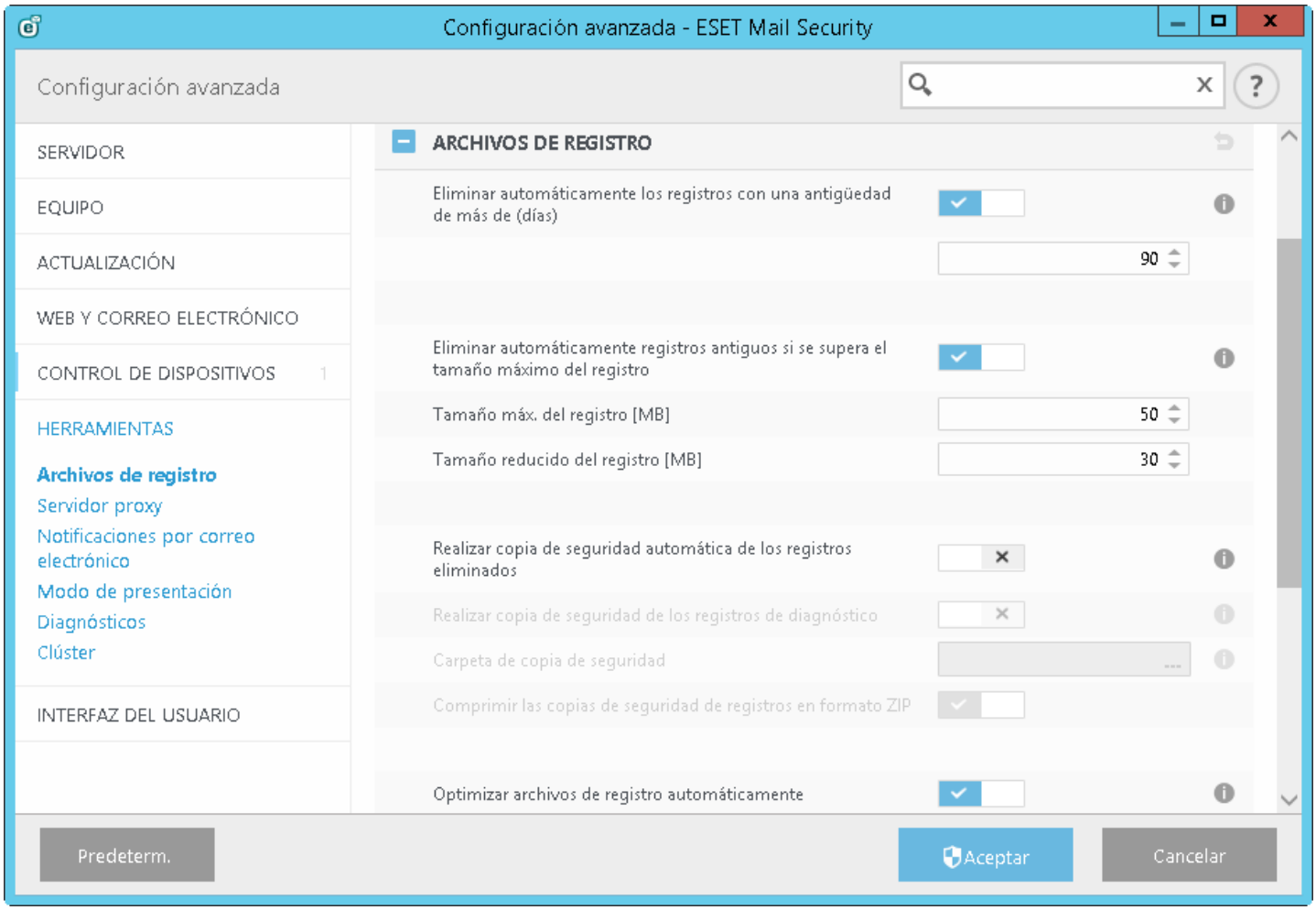
Cuando se activa la función **Generar lista de objetos**, ESET Mail Security crea una lista de objetos de análisis disponibles actualmente. Esta lista se genera periódicamente en función del **Período de actualización** definido en minutos. Cuando ERA desee ejecutar la tarea **Análisis del servidor** cliente, recopilará la lista y le permitirá elegir objetos de análisis de base de datos a petición en ese servidor determinado.

5.6.6 Archivos de registro

Puede usar el conmutador para desactivar o activar la función **Registro de diagnóstico** del clúster. Está activada de forma predeterminada. Esto significa que el registro del clúster se incluirá en el registro de diagnóstico general. Para iniciar el registro real tendrá que activar el registro de diagnóstico general a nivel del producto en el menú principal > Configuración > Herramientas. Una vez activado, el registro de diagnóstico también recopilará registros detallados del Clúster de ESET.

El apartado **Archivos de registro** le permite modificar la configuración de registro de ESET Mail Security.

Puede definir cómo se gestionarán los registros. El programa elimina automáticamente los registros antiguos para ahorrar espacio en el disco duro.



5.6.6.1 Filtrado de registros

Los registros guardan información sobre sucesos importantes del sistema. La función de filtrado de registros permite ver los registros de un tipo de suceso determinado.

Escriba la palabra clave de búsqueda en el campo **Buscar texto**. Utilice el menú desplegable **Buscar en columnas** para limitar la búsqueda.

Tipos de registro: seleccione uno o varios tipos de registro en el menú desplegable:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus).

Período de tiempo: define el período de tiempo para el que desea visualizar los resultados.

Solo palabras completas: seleccione esta casilla de verificación si desea buscar palabras completas específicas para obtener resultados más precisos.

Distinguir mayúsculas y minúsculas: active esta opción si considera que es importante distinguir mayúsculas y minúsculas durante el filtrado.

5.6.6.2 Buscar en el registro

La opción Filtrado de registros se puede combinar con la función de búsqueda en archivos de registro, aunque esta última también se puede utilizar por separado. Esta función es útil cuando se buscan registros específicos. Al igual que el filtrado de registros, esta función de búsqueda le ayuda a encontrar la información que busca y es especialmente útil cuando hay demasiados registros.

Durante el uso de la búsqueda en el registro puede usar la opción **Buscar texto** al escribir una cadena de búsqueda concreta, emplear el menú desplegable **Buscar en columnas** para filtrar por columna, seleccionar **Tipos de registro** y establecer un **Período de tiempo** para solo buscar registros de un período de tiempo concreto. Al especificar determinadas opciones de búsqueda, en la ventana Archivos de registro solo se buscan los registros pertinentes (según estas opciones de búsqueda).

Buscar texto: escriba lo que desea buscar en una cadena de caracteres (palabra completa o parcial). Solo se buscarán los registros que contengan dicha cadena; El resto de registros se omitirán.

Buscar en columnas: seleccione las columnas que se tendrán en cuenta en la búsqueda. Puede seleccionar las columnas que desee para la búsqueda. De forma predeterminada, están seleccionadas todas las columnas:

- **Tiempo**
- **Carpeta analizada**
- **Suceso**
- **Usuario**

Tipos de registro: seleccione uno o varios tipos de registro en el menú desplegable:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus).

Período de tiempo: permite definir el período de tiempo para el que desea visualizar los resultados.

- **No especificado** (predeterminada): no busca en un período de tiempo determinado, sino en todo el registro.
- **Último día**
- **Última semana**
- **Último mes**
- **Período de tiempo**: permite especificar el período de tiempo exacto (fecha y hora) para buscar únicamente los registros correspondientes a un período de tiempo especificado.

Solo palabras completas: busca únicamente los registros que coinciden totalmente con la cadena especificada en el cuadro de texto **Qué**.

Distinguir mayúsculas y minúsculas: busca únicamente los registros que coinciden con la cadena especificada en el cuadro de texto **Qué** y utilizan las mismas mayúsculas y minúsculas.

Buscar hacia arriba: busca de la posición actual hacia arriba.

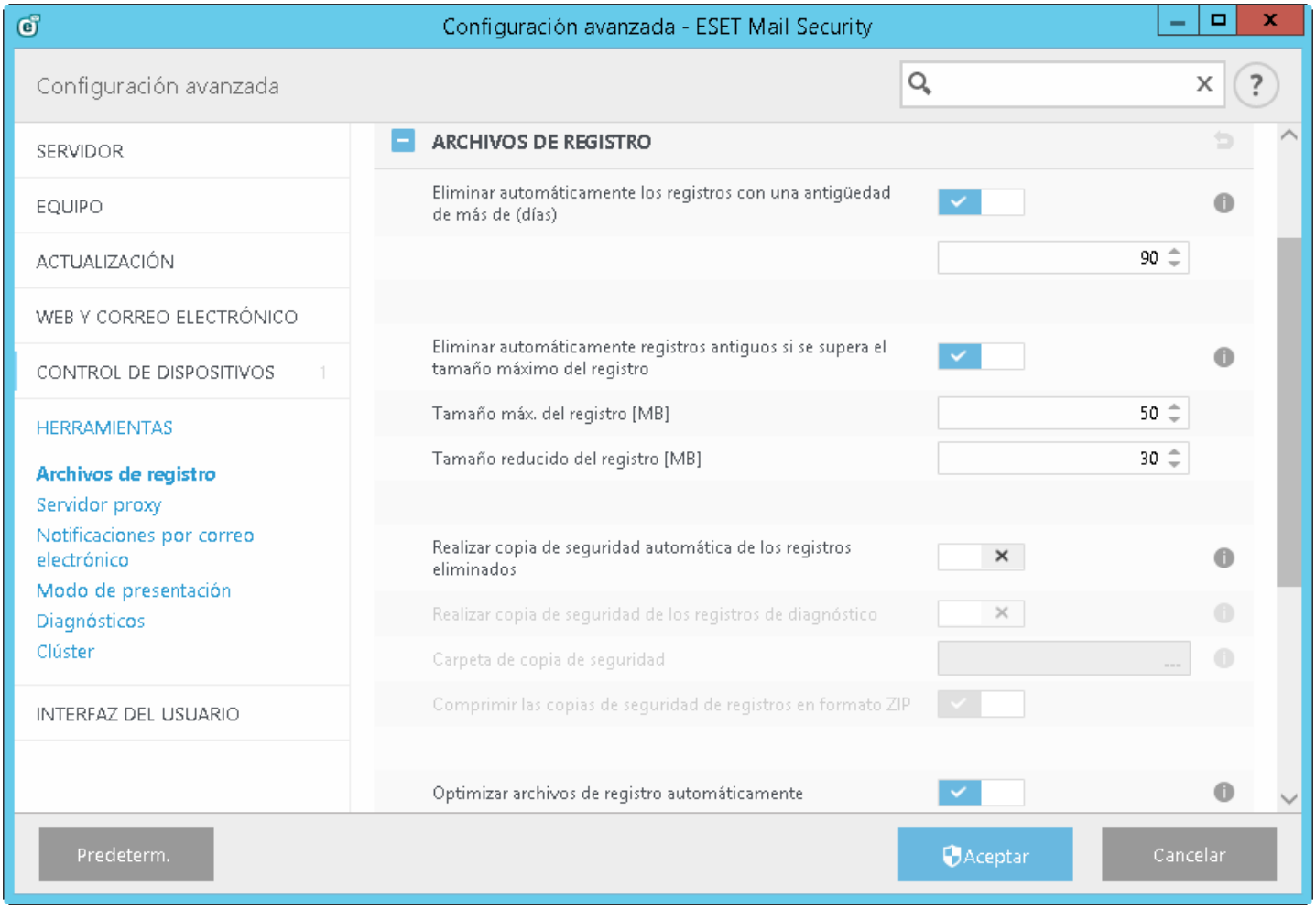
Una vez que haya configurado las opciones de búsqueda, haga clic en **Buscar** para iniciar la búsqueda. La búsqueda se detiene cuando se encuentra el primer registro coincidente. Haga clic en **Buscar** de nuevo para ver más registros. La búsqueda en los archivos de registro se realiza de arriba abajo, a partir de la posición actual (registro resaltado).

5.6.6.3 Mantenimiento de registros

Puede usar el conmutador para desactivar o activar la función **Registro de diagnóstico** del clúster. Está activada de forma predeterminada. Esto significa que el registro del clúster se incluirá en el registro de diagnóstico general. Para iniciar el registro real tendrá que activar el registro de diagnóstico general a nivel del producto en el menú principal > Configuración > Herramientas. Una vez activado, el registro de diagnóstico también recopilará registros detallados del Clúster de ESET.

El apartado **Archivos de registro** le permite modificar la configuración de registro de ESET Mail Security.

Puede definir cómo se gestionarán los registros. El programa elimina automáticamente los registros antiguos para ahorrar espacio en el disco duro.



- **Eliminar registros automáticamente**: las entradas de registro anteriores al número de días especificado se eliminan de forma automática.
- **Optimizar los archivos de registro automáticamente**: activa la desfragmentación automática de los archivos de registro si se supera el porcentaje especificado de registros sin utilizar.
- **Nivel mínimo de detalle al registrar**: especifica el nivel de detalle del registro. Opciones disponibles:
  - **Registros de diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
  - **Registros de información**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
  - **Alertas**: registra errores graves y mensajes de alerta.
  - **Errores**: solo registra los mensajes "Error al descargar el archivo" y los errores graves.
  - **Alertas críticas**: solo registra los errores graves (errores al iniciar la protección antivirus, etc.).

5.6.7 Servidor proxy

En las redes LAN de gran tamaño, un servidor Proxy puede mediar en la conexión del ordenador a Internet. Si este es el caso, es necesario definir los siguientes ajustes. De lo contrario, el programa no se podrá actualizar de manera automática. En ESET Mail Security, el servidor proxy se puede configurar en dos secciones diferentes del árbol de configuración avanzada.

En primer lugar, se puede configurar en **Configuración avanzada**, bajo **Herramientas** > **Servidor proxy**. Al especificar el servidor proxy en este nivel se define la configuración global del servidor proxy para ESET Mail Security. Todos los módulos que requieran conexión a Internet utilizarán estos parámetros.

Para especificar la configuración del servidor proxy en este nivel, active el conmutador **Usar servidor proxy** y, a continuación, especifique la dirección del servidor proxy en el campo **Servidor proxy** y su número de **Puerto**.

Si la comunicación con el servidor proxy requiere autenticación, active el conmutador **El servidor proxy requiere autenticación** e introduzca un **Nombre de usuario** y una **Contraseña** válidos en los campos correspondientes. Haga clic en **Detectar** para detectar y cumplimentar la configuración del servidor proxy de forma automática. Se copiarán los parámetros especificados en Internet Explorer.

NOTA: esta función no recupera los datos de autenticación (nombre de usuario y contraseña), de modo que el usuario debe proporcionarlos.

La configuración del servidor proxy también se puede definir en Configuración avanzada de actualizaciones (**Configuración avanzada** > **Actualización** > **Proxy HTTP**; para ello, seleccione **Conexión a través de un servidor proxy** en el menú desplegable **Modo proxy**). Esta configuración se aplica al perfil de actualización dado, y se recomienda para ordenadores portátiles que suelen recibir actualizaciones de firmas de virus de diferentes ubicaciones. Para obtener más información sobre esta configuración, consulte la sección Configuración avanzada de actualizaciones.

5.6.8 Notificaciones por correo electrónico

ESET Mail Security puede enviar correos electrónicos de forma automática si se produce un suceso con el nivel de detalle seleccionado. Active **Enviar notificaciones de sucesos por correo electrónico** para activar las notificaciones por correo electrónico.

NOTA: los servidores SMTP con cifrado TLS son compatibles con ESET Mail Security.

- **Servidor SMTP**: el servidor SMTP utilizado para enviar notificaciones.
- **Nombre de usuario y contraseña**: si el servidor SMTP requiere autenticación, estos campos deben cumplimentarse con un nombre de usuario y una contraseña válidos que faciliten el acceso al servidor SMTP.
- **Dirección del remitente**: introduzca la dirección del remitente que aparecerá en el encabezado de los correos electrónicos de notificación. Esto es lo que el destinatario verá como **De**.
- **Dirección del destinatario**: especifique la dirección de correo electrónico del destinatario **Para** al que se entregarán las notificaciones.
- **Nivel mínimo de detalle para las notificaciones**: especifica el nivel mínimo de detalle de las notificaciones que se van a enviar.
- **Habilitar TLS**: active el envío de mensajes de notificación y alerta que admite el cifrado TLS.
- **Intervalo tras el que se enviarán nuevos correos electrónicos de notificación (min)**: intervalo en minutos tras el cual se enviarán nuevas notificaciones mediante correo electrónico. Si desea que estas notificaciones se envíen inmediatamente, ajuste este valor a 0.
- **Enviar cada notificación en un correo electrónico distinto**: si esta opción está activada, el destinatario recibirá un correo electrónico nuevo para cada notificación. Esto podría suponer la recepción de numerosos correos electrónicos en un breve periodo de tiempo.

Formato de mensajes

- **Para notificar la ocurrencia de sucesos**: formato de los mensajes de suceso que se muestran en los ordenadores remotos. Consulte también Modificar formato.
- **Para alertar sobre amenazas**: los mensajes de notificación y alerta de amenazas tienen un formato predefinido de

forma predeterminada. Le aconsejamos que no modifique este formato. No obstante, en algunas circunstancias (por ejemplo, si tiene un sistema automatizado de procesamiento de correo electrónico), es posible que deba modificar el formato de los mensajes. Consulte también Modificar formato.

- **Usar caracteres del alfabeto local**: convierte un mensaje de correo electrónico a la codificación de caracteres ANSI basándose en la configuración regional de Windows (p. ej., windows-1250). Si deja esta opción sin marcar, se convertirá y codificará un mensaje en ASCII de 7 bits (por ejemplo, "á" se cambiará a "a", y un símbolo desconocido a "?").
- **Usar la codificación local de caracteres**: el origen del mensaje de correo electrónico se codificará a formato Quoted-printable (QP), que utiliza caracteres ASCII y solo pude transmitir correctamente caracteres nacionales especiales por correo electrónico en formato de 8 bits (ááíóú).

5.6.8.1 Formato de mensajes

Las comunicaciones entre el programa y un usuario o administrador de sistemas remotos se realizan a través de mensajes de correo electrónico o mensajes de red local (mediante el servicio de mensajería de Windows®). El formato predeterminado de los mensajes de alerta y las notificaciones será el óptimo para la mayoría de situaciones. En algunas circunstancias, tendrá que cambiar el formato de los mensajes de sucesos.

Las palabras clave (cadenas separadas por signos %) se sustituyen en el mensaje por la información real especificada. Están disponibles las siguientes palabras clave:

- **%TimeStamp%**: fecha y hora del suceso.
- **%Scanner%**: módulo correspondiente.
- **%ComputerName%**: nombre del ordenador en el que se produjo la alerta.
- **%ProgramName%**: programa que generó la alerta.
- **%InfectedObject%**: nombre del archivo, mensaje, etc., infectado.
- **%VirusName%**: identificación de la infección.
- **%ErrorDescription%**: descripción de un suceso que no está relacionado con un virus.

Las palabras clave **%InfectedObject%** y **%VirusName%** solo se utilizan en los mensajes de alerta de amenaza y **%ErrorDescription%**, en los mensajes de sucesos.

5.6.9 Modo de presentación

El modo de presentación es una característica para usuarios que exigen un uso del software sin interrupciones y sin ventanas emergentes, así como un menor uso de la CPU. Este modo también se puede utilizar para que las presentaciones no se vean interrumpidas por la actividad del módulo antivirus. Cuando está activado, se desactivan todas las ventanas emergentes y las tareas programadas no se ejecutan. La protección del sistema sigue ejecutándose en segundo plano, pero no requiere la intervención del usuario.

Haga clic en **Configuración** > **Ordenador** y, a continuación, haga clic en el conmutador situado junto a **Modo de presentación** para activarlo de forma manual. En **Configuración avanzada** (F5), haga clic en **Herramientas** > **Modo de presentación** y, a continuación, haga clic en el conmutador situado junto a **Activar el modo de presentación automáticamente, al ejecutar aplicaciones en modo de pantalla completa** para que ESET Mail Security active este modo automáticamente cuando se ejecuten aplicaciones a pantalla completa. Activar el modo de presentación constituye un riesgo de seguridad potencial, por lo que el icono de estado de la protección disponible en la barra de tareas se volverá naranja y mostrará un signo de alerta. Esta alerta también se puede ver en la ventana principal del programa donde verá el mensaje **El modo de presentación está activado** en naranja.

Si selecciona **Activar el modo de presentación automáticamente, al ejecutar aplicaciones en modo de pantalla completa**, el modo de presentación se activará cuando inicie una aplicación a pantalla completa y se detendrá automáticamente cuando cierre dicha aplicación. Esta función es muy útil para que el modo de presentación se inicie de inmediato al empezar un juego, abrir una aplicación a pantalla completa o iniciar una presentación.

También puede seleccionar **Desactivar el modo de presentación automáticamente después de** para definir la cantidad de tiempo, en minutos, que tardará en desactivar el modo de presentación automáticamente.

5.6.10 Diagnóstico

El diagnóstico proporciona volcados de memoria de los procesos de ESET (por ejemplo, *ekrn*). Cuando una aplicación se bloquea, se genera un volcado de memoria que puede ayudar a los desarrolladores a depurar y arreglar varios problemas de ESET Mail Security. Haga clic en el menú desplegable situado junto a **Tipo de volcado** y seleccione una de las tres opciones disponibles:

- Seleccione **Desactivar** (predeterminada) para desactivar esta función.
- **Mini**: registra la información mínima necesaria para identificar el motivo del bloqueo inesperado de la aplicación. Este tipo de volcado puede resultar útil cuando el espacio es limitado. Sin embargo, dada la poca información que proporciona, es posible que el análisis de este archivo no detecte los errores que no estén relacionados directamente con el subproceso que se estaba ejecutando cuando se produjo el problema.
- **Completo**: registra todo el contenido de la memoria del sistema cuando la aplicación se detiene de forma inesperada. Los volcados de memoria completos pueden contener datos de procesos que se estaban ejecutando cuando se generó el volcado.

Directorio de destino: directorio en el que se genera el volcado durante el bloqueo.

Abrir la carpeta de diagnóstico: haga clic en **Abrir** para abrir este directorio en una ventana nueva del *Explorador de Windows*.

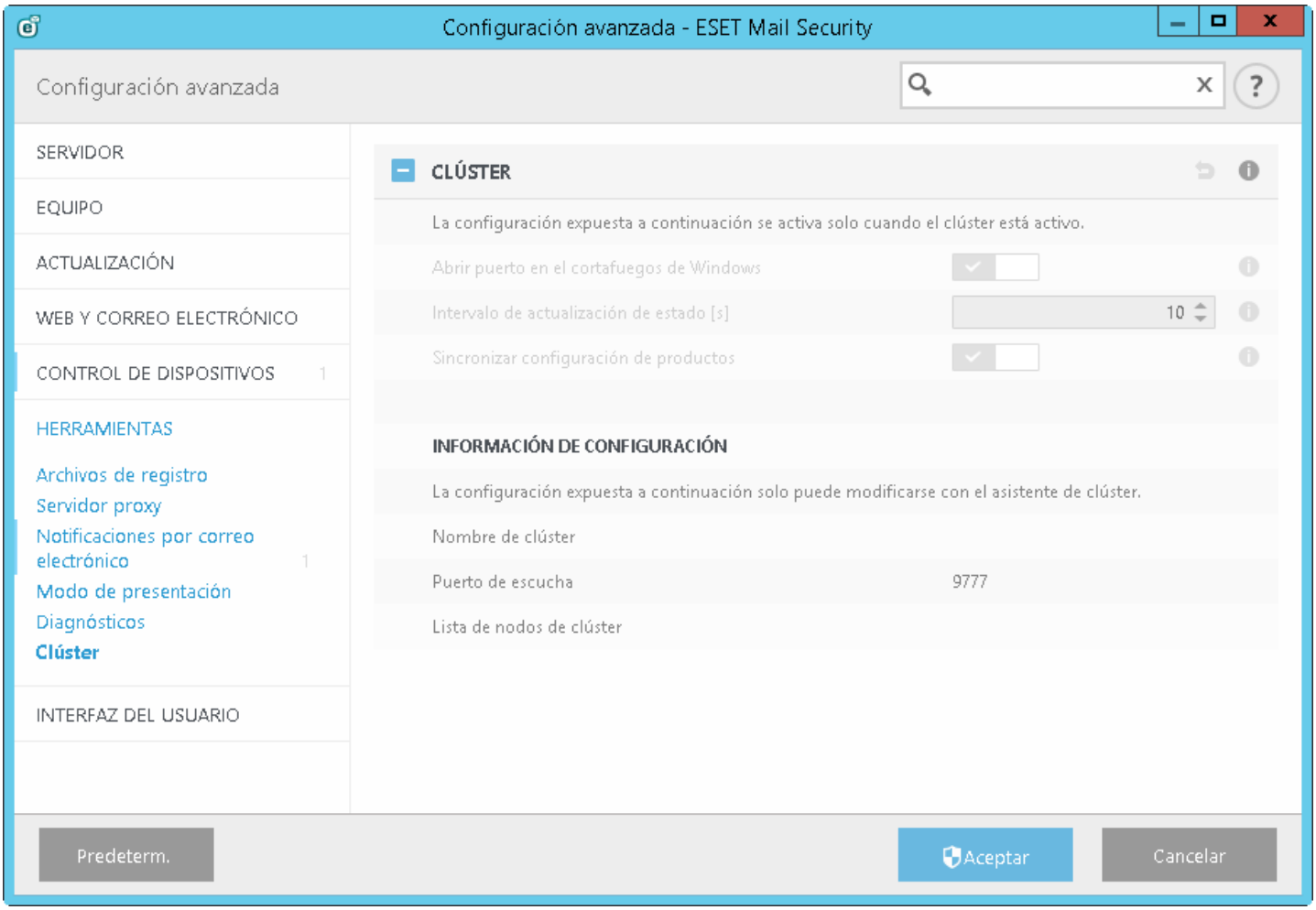
5.6.11 Atención al cliente

Enviar datos de configuración del sistema: seleccione **Enviar siempre** en el menú desplegable o **Preguntar antes de enviar** para que se le pregunte antes de que se envíen los datos.

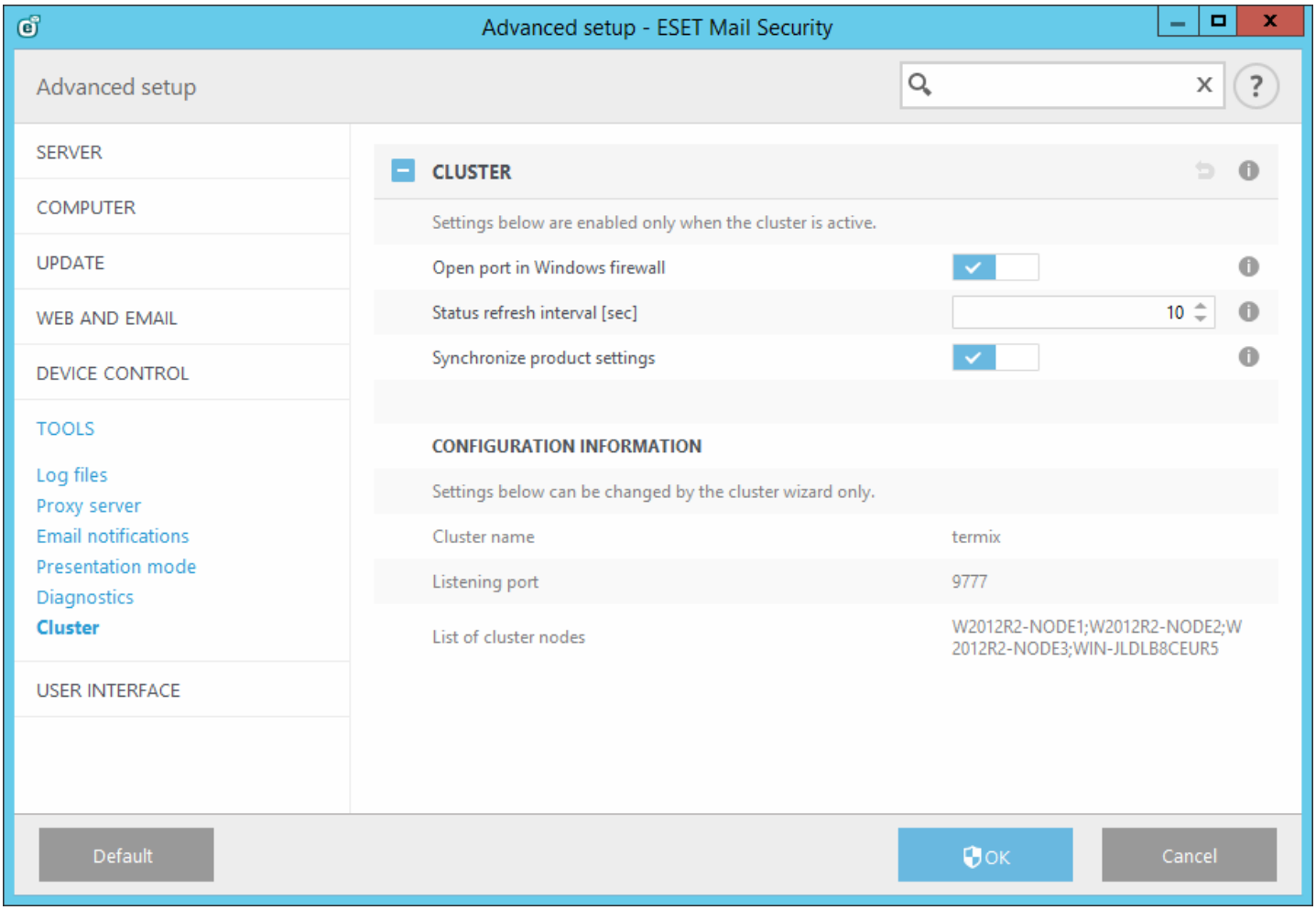
5.6.12 Clúster

La opción **Activar clúster** se activa automáticamente cuando se configura el Clúster de ESET. Puede desactivarla manualmente en la ventana de Configuración avanzada; para ello haga clic en el icono del conmutador (es una opción idónea cuando necesita cambiar la configuración sin que esto tenga consecuencias sobre el resto de nodos del Clúster de ESET). Este conmutador solo activa o desactiva la funcionalidad Clúster de ESET. Para configurar correctamente o destruir el clúster, se debe usar el Asistente de clúster o la opción Destruir clúster de la sección **Herramientas** > **Clúster** de la ventana principal del programa.

Clúster de ESET no configurado y desactivado:



Clúster de ESET correctamente configurado con sus detalles y opciones:



Si desea obtener más información sobre el Clúster de ESET, haga clic aquí.

5.7 Interfaz de usuario

En la sección **Interfaz de usuario** es posible configurar el comportamiento de la interfaz gráfica de usuario (GUI) del programa. Es posible ajustar el aspecto y los efectos visuales del programa.

Si desea disponer del máximo nivel de seguridad del software de seguridad, utilice la herramienta Configuración de acceso para impedir los cambios no autorizados.

En la configuración de Alertas y notificaciones, puede cambiar el comportamiento de las alertas de amenaza detectadas y las notificaciones del sistema, que se pueden adaptar a las necesidades de cada uno.

Si elige la opción de no mostrar algunas notificaciones, estas se mostrarán en el área Mensajes y estados desactivados. Aquí puede comprobar su estado, ver más información o eliminarlas de esta ventana.

La opción Integración en el menú contextual aparece al hacer clic con el botón derecho en el objeto seleccionado. Utilice esta herramienta para integrar elementos de control de ESET Mail Security en el menú contextual.

El modo Presentación es útil para usuarios que deseen trabajar con una aplicación sin la interrupción de ventanas emergentes, tareas programadas y cualquier componente que podría exigir gran cantidad de recursos del sistema.

Elementos de la interfaz del usuario

Las opciones de configuración de la interfaz de usuario de ESET Mail Security le permiten ajustar el entorno de trabajo según sus necesidades. Estas opciones de configuración están disponibles en la sección **Interfaz de usuario** > **Elementos de la interfaz del usuario** del árbol de configuración avanzada de ESET Mail Security.

En la sección **Elementos de la interfaz del usuario** puede ajustar el entorno de trabajo. Si los elementos gráficos ralentizan el ordenador o provocan otros problemas, establezca Interfaz de usuario en **Terminal**. También se

recomienda desactivar la interfaz gráfica de usuario en un Terminal Server. Si desea obtener más información sobre la instalación de ESET Mail Security en un Terminal Server, consulte el tema Desactivar la GUI en Terminal Server.

Haga clic en el menú desplegable **Modo de inicio** para seleccionar uno de los siguientes modos de inicio:
- **Completo**: se muestra la GUI completa.
- **Terminal**: no se muestra ninguna notificación ni alerta. La GUI solo la puede iniciar el administrador.

Si desea desactivar la pantalla inicial de ESET Mail Security, anule la selección de **Mostrar pantalla inicial con la carga del sistema**.

Si desea que ESET Mail Security reproduzca un sonido cuando se produzcan sucesos importantes durante un análisis, por ejemplo al detectar una amenaza o al finalizar el análisis, seleccione **Usar señal acústica**.

Integrar el programa dentro del menú contextual: integre los elementos de control de ESET Mail Security en el menú contextual.

Estados: haga clic en Editar para administrar (activar o desactivar) los estados que se muestran en el panel Supervisión del menú principal. **Estados de la aplicación**: le permite activar o desactivar el estado de visualización en el panel **Estado de protección** del menú principal.

Información de la licencia: esta opción le permite ver información, mensajes y notificaciones relacionados con la licencia.

5.7.1 Alertas y notificaciones

La sección de **Alertas y notificaciones** de **Interfaz de usuario** le permite configurar cómo gestiona ESET Mail Security las notificaciones del sistema (por ejemplo, mensajes de actualización correcta) y las alertas de amenaza. También puede definir si se muestra la hora y la transparencia de las notificaciones de la bandeja del sistema (esto se aplica únicamente a los sistemas que admiten notificaciones en la bandeja del sistema).

Ventanas de alerta

Si desactiva la opción **Mostrar alertas**, se cancelarán todos los mensajes de alerta. Solo resulta útil para una serie de situaciones muy específicas. Para la mayoría de los usuarios, se recomienda mantener la configuración predeterminada (activada).

Notificaciones en el escritorio

Las notificaciones del escritorio y los globos de sugerencias son medios de información que no requieren la intervención del usuario. Se muestran en el área de notificación, situada en la esquina inferior derecha de la pantalla. Para activar las notificaciones de escritorio, seleccione **Mostrar notificaciones en el escritorio**. A continuación encontrará más opciones avanzadas, como la modificación del tiempo de visualización de las notificaciones y la transparencia de las ventanas.

Active el conmutador **No mostrar las notificaciones al ejecutar aplicaciones en modo de pantalla completa** para suprimir todas las notificaciones que no sean interactivas.

En el menú desplegable **Nivel mínimo de detalle de los sucesos a mostrar**, se puede seleccionar el nivel de gravedad de las alertas y notificaciones que se mostrarán. Están disponibles las opciones siguientes:

- **Diagnóstico**: registra la información necesaria para ajustar el programa y todos los registros anteriores.
- **Informativo**: registra los mensajes informativos, incluidos los mensajes de las actualizaciones realizadas con éxito y todos los registros anteriores.
- **Alertas**: registra errores graves y mensajes de alerta.
- **Errores**: se registran los errores graves y errores del tipo "Error al descargar el archivo".
- **Críticos**: registra únicamente los errores graves (errores al iniciar la protección antivirus, etc.).

La última característica de esta sección le permite configurar el destino de las notificaciones en un entorno con varios usuarios. En el campo **En sistemas con varios usuarios, mostrar las notificaciones en la pantalla de este usuario** se especifica el usuario que recibirá notificaciones del sistema y de otro tipo en sistemas que permitan la conexión de varios usuarios al mismo tiempo. Normalmente, este usuario es un administrador de sistemas o de redes. Esta opción resulta especialmente útil para servidores de terminal, siempre que todas las notificaciones del

sistema se envíen al administrador.

Cuadros de mensajes

Para cerrar las ventanas emergentes automáticamente después de un período de tiempo determinado, seleccione la opción **Cerrar ventanas de notificación automáticamente**. Si no se cierran de forma manual, las ventanas de alerta se cerrarán automáticamente cuando haya transcurrido el periodo de tiempo especificado.

5.7.2 Configuración de acceso

Para ofrecer la máxima seguridad a su sistema, es esencial que ESET Mail Security se haya configurado correctamente. Una configuración incorrecta puede provocar la pérdida de datos importantes. Para evitar modificaciones no autorizadas, los parámetros de configuración de ESET Mail Security se pueden proteger mediante contraseña. Las opciones de configuración para la protección mediante contraseña se encuentran en el submenú **Configuración de acceso**, en la sección **Interfaz de usuario** del árbol de configuración avanzada.

Protección de la configuración: bloquea o desbloquea los parámetros de configuración del programa. Haga clic para abrir la ventana de configuración de contraseña.

Para configurar o cambiar una contraseña con el fin de proteger los parámetros de configuración, haga clic en **Introduzca la contraseña**.

Exigir derechos de administrador completos a las cuentas de administrador limitadas: seleccione esta opción para solicitar al usuario actual (si no tiene derechos de administrador) que introduzca el nombre de usuario y la contraseña de administrador al modificar determinados parámetros del sistema (parecido al UAC en Windows Vista). Estas modificaciones incluyen la desactivación de los módulos de protección.

5.7.2.1 Contraseña

Para evitar modificaciones no autorizadas, los parámetros de configuración de ESET Mail Security se pueden proteger mediante contraseña.

5.7.2.2 Configuración de la contraseña

Debe definir una nueva contraseña para proteger los parámetros de configuración de ESET Mail Security con el fin de evitar modificaciones no autorizadas. Si desea cambiar una contraseña, escriba la contraseña actual en el campo **Contraseña anterior**, escriba la nueva contraseña en los campos **Contraseña nueva** y **Confirmar contraseña**; a continuación, haga clic en **Aceptar**. Esta contraseña es necesaria para realizar modificaciones en ESET Mail Security.

5.7.3 Ayuda

Al pulsar la tecla **F1** y el botón **?** se abre la ventana de la ayuda en línea. Esta es la fuente principal de contenido de ayuda. No obstante, junto con el programa se instala una copia sin conexión de la ayuda, que resulta útil en aquellos casos en los que no se dispone de conexión a Internet.

Siempre que tenga una conexión a Internet activa se mostrará la versión más reciente de la ayuda en línea.

5.7.4 ESET Shell

Puede configurar los derechos de acceso a la modificación del producto, sus funciones y los datos que contiene desde eShell, mediante la modificación de la **Directiva de ejecución de ESET Shell**. El ajuste predeterminado es **Scripts limitados**, pero puede cambiarlo a **Desactivado**, **Solo lectura** o **Acceso total** en caso de ser necesario.

- **Desactivado**: eShell no puede usarse. Solo se permite la configuración de eShell en el contexto de `ui eshell`. Puede personalizar la apariencia de eShell, pero no puede acceder a ningún ajuste ni dato del producto.
- **Solo lectura**: eShell puede usarse como herramienta de supervisión. Puede ver todos los ajustes en el modo interactivo y por lotes, pero no puede modificar ningún ajuste, función ni dato.
- **Scripts limitados**: en el modo interactivo puede ver y modificar todos los ajustes, funciones y datos. En el modo por lotes, eShell funcionará como si estuviera en el modo de solo lectura. Sin embargo, si usa archivos por lotes firmados, podrá editar la configuración y modificar los datos.

- **Acceso total**: ofrece acceso a todos los ajustes de forma ilimitada, en el modo tanto interactivo como por lotes. Puede consultar y modificar cualquier ajuste. Debe usar una cuenta de administrador para ejecutar eShell con acceso total. Si el Control de cuentas de usuario está activado, también se requiere elevación.

5.7.5 Desactivar la GUI en Terminal Server

En este capítulo se explica cómo desactivar la ejecución de la GUI de ESET Mail Security en Windows Terminal Server para las sesiones de usuario.

Normalmente, la GUI de ESET Mail Security se inicia cada vez que un usuario remoto inicia sesión en el servidor y crea una sesión de Terminal; una acción que no suele ser deseable en los servidores Terminal Server. Si desea desactivar la GUI en las sesiones de terminal, puede hacerlo desde eShell mediante la ejecución del comando `set ui ui gui-start-mode terminal`. De esta forma activará el modo terminal en la GUI. Estos son los dos modos disponibles para el inicio de la GUI:

```
set ui ui gui-start-mode full
set ui ui gui-start-mode terminal
```

Si desea averiguar qué modo se está usando actualmente, ejecute el comando `get ui ui gui-start-mode`.

NOTA: si ha instalado ESET Mail Security en un servidor Citrix, se recomienda utilizar la configuración descrita en el artículo de nuestra base de conocimiento.

5.7.6 Mensajes y estados desactivados

Mensajes de confirmación: muestra una lista de mensajes de confirmación que se pueden seleccionar para que se muestren o no.

Estados de aplicación desactivados: le permite activar o desactivar el estado de visualización en el panel **Estado de protección** del menú principal.

5.7.6.1 Mensajes de confirmación

En este cuadro de diálogo se muestran los mensajes de confirmación que mostrará ESET Mail Security antes de que se realice cualquier acción. Seleccione o anule la selección de la casilla de verificación disponible junto a cada mensaje de confirmación para permitirlo o desactivarlo.

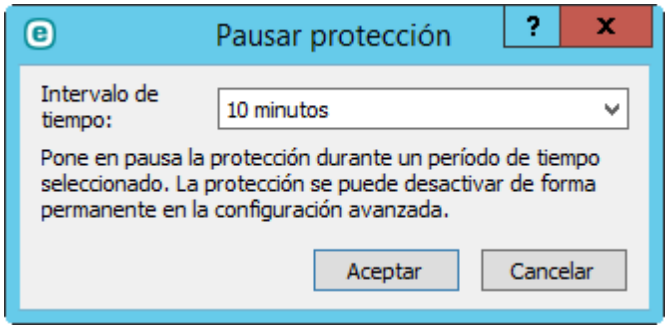
5.7.6.2 Estados de aplicación desactivados

En este cuadro de diálogo puede seleccionar o anular la selección de los estados de aplicación que desea que se muestren o no. Por ejemplo, cuando pone en pausa la protección antivirus y antiespía o cuando activa el modo de presentación. El estado de una aplicación también se muestra cuando no se ha activado el producto o si la licencia ha expirado.

5.7.7 Icono en la bandeja del sistema

Algunas de las opciones y características de configuración más importantes están disponibles al hacer clic con el botón derecho del ratón en el icono de la bandeja del sistema.

Pausar protección: muestra el cuadro de diálogo de confirmación que desactiva la Protección antivirus y antiespía, que protege el sistema frente a ataques mediante el control de archivos, Internet y la comunicación por correo electrónico.


Pausar protección
Intervalo de tiempo:
10 minutos
Pone en pausa la protección durante un período de tiempo seleccionado. La protección se puede desactivar de forma permanente en la configuración avanzada.
Aceptar
Cancelar

En el menú desplegable **Intervalo de tiempo** se indica el período de tiempo durante el que estará desactivada la protección antivirus y antiespía.

Configuración avanzada: seleccione esta opción para acceder al árbol de **Configuración avanzada**. También puede acceder a Configuración mediante la tecla F5 o desde **Configuración** > **Configuración avanzada**.

Archivos de registro: los archivos de registro contienen información acerca de todos los sucesos importantes del programa y proporcionan información general acerca de las amenazas detectadas.

Ocultar ESET Mail Security: oculta la ventana de ESET Mail Security.

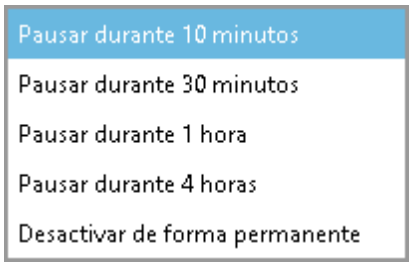
Restablecer disposición de la ventana: esta opción restablece el tamaño y la posición predeterminados de la ventana de ESET Mail Security.

Actualización de la base de firmas de virus: actualiza la base de firmas de virus para garantizar el nivel de protección frente a código malicioso.

Acerca de: proporciona información del sistema y detalles acerca de la versión instalada de ESET Mail Security, así como de los módulos del programa instalados y la fecha de caducidad de la licencia. Al final de la página encontrará información sobre el sistema operativo y los recursos del sistema.

5.7.7.1 Pausar la protección

Cuando pause temporalmente la protección antivirus y antiespía con el icono de la bandeja del sistema, aparecerá el cuadro de diálogo **Pausar la protección de forma temporal**. Al hacerlo se desactivará la protección relacionada con el código malicioso durante el periodo de tiempo seleccionado (para desactivar la protección de forma permanente debe hacerlo desde Configuración avanzada). Tenga cuidado, ya que desactivar la protección puede exponer su sistema a amenazas.

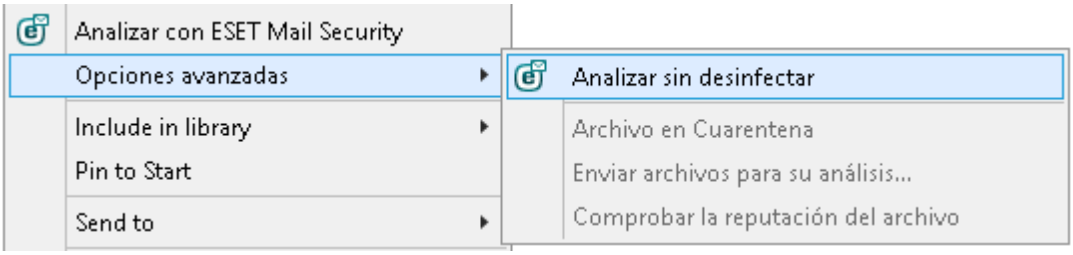

Pausar durante 10 minutos
Pausar durante 30 minutos
Pausar durante 1 hora
Pausar durante 4 horas
Desactivar de forma permanente

5.7.8 Menú contextual

El menú contextual aparece al hacer clic con el botón derecho en un objeto (archivo). En el menú se muestra una lista de todas las acciones que se pueden realizar en un objeto.

Es posible integrar elementos de control de ESET Mail Security en el menú contextual. El árbol de configuración avanzada contiene una opción de configuración de esta función, en **Interfaz de usuario** > **Elementos de la interfaz del usuario**.

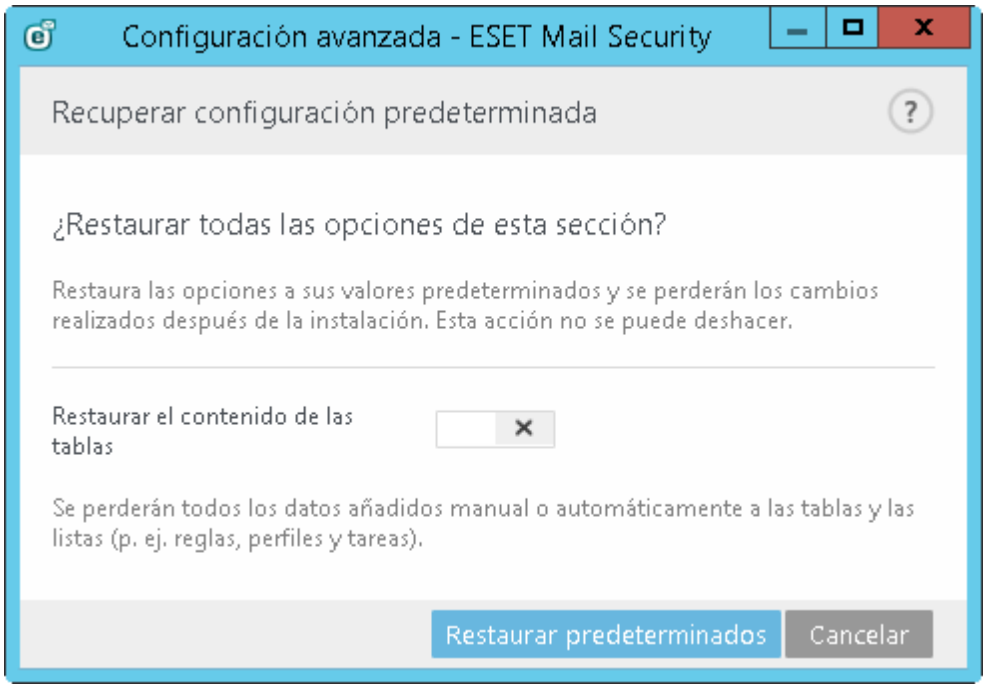
Integrar el programa dentro del menú contextual: integre los elementos de control de ESET Mail Security en el menú contextual.



5.8 Restaurar la configuración de esta sección

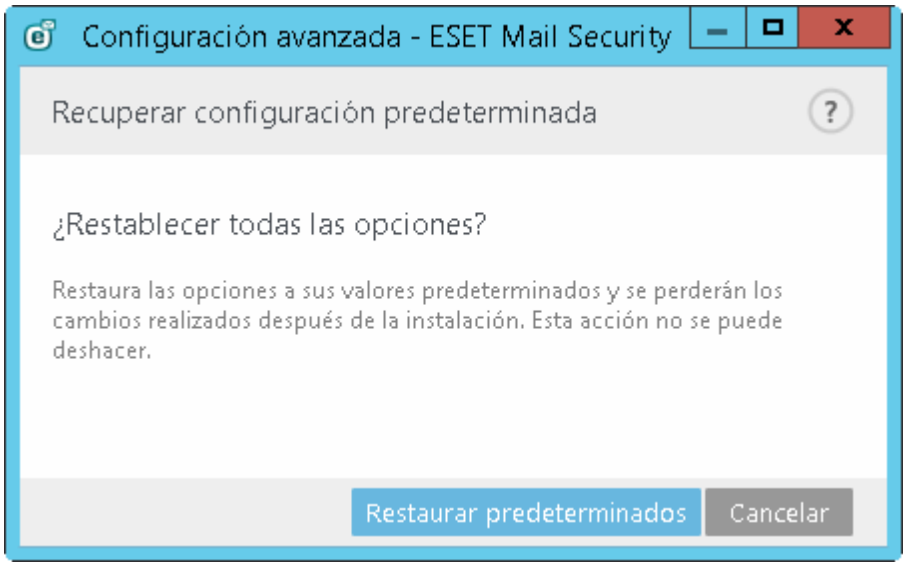
Restablece la configuración del módulo a los valores predeterminados de ESET. Tenga en cuenta que, al hacer clic en **Restaurar predeterminados**, se perderán todos los cambios realizados.

Restaurar el contenido de las tablas: si está activada, se perderán las reglas, tareas o perfiles que se hayan añadido de forma manual o automática.


Configuración avanzada - ESET Mail Security
Recuperar configuración predeterminada
¿Restaurar todas las opciones de esta sección?
Restaura las opciones a sus valores predeterminados y se perderán los cambios realizados después de la instalación. Esta acción no se puede deshacer.
Restaurar el contenido de las tablas
Se perderán todos los datos añadidos manual o automáticamente a las tablas y las listas (p. ej. reglas, perfiles y tareas).
Restaurar predeterminados
Cancelar

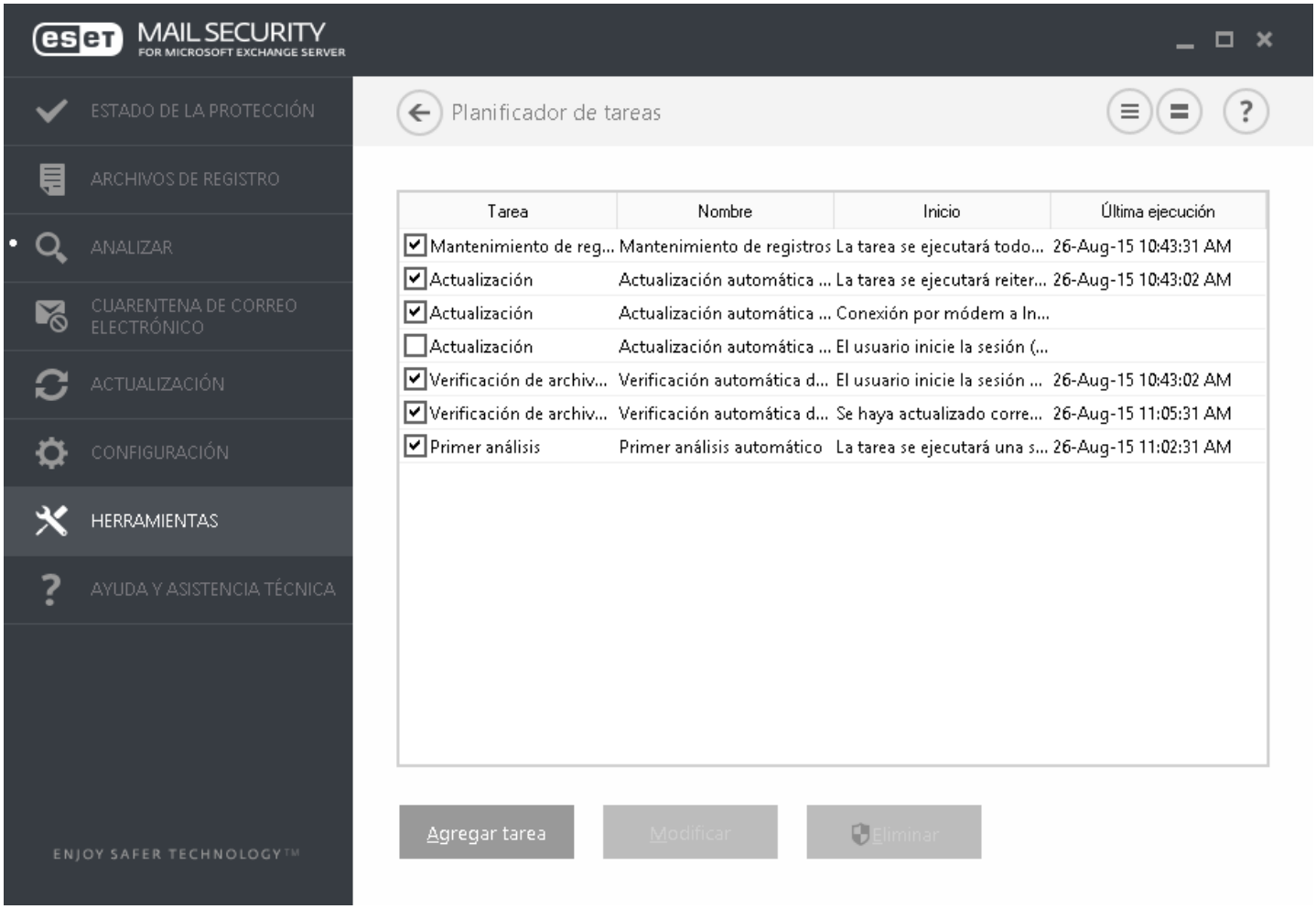
5.9 Restaurar la configuración predeterminada

Se restablecerá toda la configuración, de todos los módulos, al estado que tendría después de una nueva instalación.


Configuración avanzada - ESET Mail Security
Recuperar configuración predeterminada
¿Restablecer todas las opciones?
Restaura las opciones a sus valores predeterminados y se perderán los cambios realizados después de la instalación. Esta acción no se puede deshacer.
Restaurar predeterminados
Cancelar

5.10 Tareas programadas

El **Planificador de tareas** se puede encontrar en el menú principal de ESET Mail Security, en **Herramientas**, y contiene una lista de todas las tareas programadas y sus propiedades de configuración, como la fecha, la hora y el perfil de análisis predefinidos utilizados.


MAIL SECURITY
FOR MICROSOFT EXCHANGE SERVER
ESTADO DE LA PROTECCIÓN
ARCHIVOS DE REGISTRO
ANALIZAR
CUARENTENA DE CORREO ELECTRÓNICO
ACTUALIZACIÓN
CONFIGURACIÓN
HERRAMIENTAS
AYUDA Y ASISTENCIA TÉCNICA
ENJOY SAFER TECHNOLOGY™
Planificador de tareas
Tarea
Nombre
Inicio
Última ejecución
Mantenimiento de reg... Mantenimiento de registros La tarea se ejecutará todo... 26-Aug-15 10:43:31 AM
Actualización Actualización automática ... La tarea se ejecutará reiter... 26-Aug-15 10:43:02 AM
Actualización Actualización automática ... Conexión por módem a In...
Actualización Actualización automática ... El usuario inicie la sesión (...
Verificación de archiv... Verificación automática d... El usuario inicie la sesión ... 26-Aug-15 10:43:02 AM
Verificación de archiv... Verificación automática d... Se haya actualizado corre... 26-Aug-15 11:05:31 AM
Primer análisis Primer análisis automático La tarea se ejecutará una s... 26-Aug-15 11:02:31 AM
Agregar tarea
Modificar
Eliminar

De forma predeterminada, en el **Planificador de tareas** se muestran las siguientes tareas programadas:

- **Mantenimiento de registros**
- **Actualización automática de rutina**
- **Actualización automática al detectar la conexión por módem**
- **Actualización automática después del registro del usuario**
- **Verificación de la ejecución de archivos en el inicio (tras el registro del usuario)**
- **Verificación de la ejecución de archivos en el inicio (tras la correcta actualización de la base de firmas de virus)**
- **Primer análisis automática**

Para modificar la configuración de una tarea programada existente (tanto predeterminada como definida por el usuario), haga clic con el botón derecho en la tarea y, a continuación, haga clic en **Modificar**; o seleccione la tarea que desea modificar y haga clic en el botón **Modificar**.

5.10.1 Detalles de la tarea

Introduzca el nombre de la tarea y selecciona una de las opciones de **Tipo de tarea**; a continuación, haga clic en **Siguiente**:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos de inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector, recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador a petición**: analiza los archivos y las carpetas del ordenador.
- **Primer análisis**: de forma predeterminada, 20 minutos después de la instalación o el reinicio se realizará un análisis del ordenador como una tarea de prioridad baja.
- **Actualizar**: programa una tarea de actualización mediante la actualización de la base de firmas de virus y los módulos del programa.
- **Análisis de base de datos**: le permite programar el análisis de una base de datos y elegir los elementos que se analizarán. Se trata básicamente de un Análisis de la base de datos a petición.

NOTA: si tiene activada la Protección de la base de datos de buzones, podrá seguir programando esta tarea, pero finalizará con el siguiente mensaje de error que aparecerá en la sección Análisis de la interfaz gráfica de usuario principal: Análisis de base de datos: el análisis se ha interrumpido debido a un error. Para evitarlo, deberá asegurarse de que la Protección de la base de datos de buzones esté desactivada durante el tiempo de ejecución del **Análisis de base de datos**.

- **Enviar informes de cuarentena de correo electrónico**: programa el envío por correo electrónico de un informe de la Cuarentena de correo electrónico.
- **Análisis en segundo plano**: ofrece a Exchange Server la oportunidad de ejecutar un análisis en segundo plano de la base de datos si fuera necesario.

- Active el conmutador **Activado** si desea activar la tarea (puede hacerlo más adelante mediante la casilla de verificación situada en la lista de tareas programadas).
- Haga clic en **Siguiente** y seleccione una de las opciones de programación: Una vez, Reiteradamente, Diariamente, Semanalmente y Cuando se cumpla la condición. Según la frecuencia seleccionada, se le solicitarán diferentes parámetros de actualización.
- La tarea **no se ejecutará si el ordenador está funcionando con batería** o está apagado.
- **A continuación**, defina la acción que debe llevarse a cabo si la tarea no se puede realizar o completar a la hora programada.

En el paso siguiente se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente. Haga clic en **Finalizar** cuando haya terminado de hacer cambios.

5.10.2 Repetición de la tarea: Una vez

Ejecución de la tarea: la tarea especificada solo se ejecutará una vez a la fecha y la hora especificadas.

5.10.3 Repetición de la tarea

La tarea se repetirá con el intervalo de tiempo especificado. Seleccione una de las opciones de programación:

- **Una vez**: la tarea se ejecutará solo una vez en la fecha y a la hora predefinidas.
- **Reiteradamente**: la tarea se ejecutará en el intervalo especificado (en horas).
- **Diariamente**: la tarea se ejecutará todos los días a la hora especificada.
- **Semanalmente**: la tarea se ejecutará una o varias veces por semana, en los días y a la hora seleccionados.
- **Cuando se cumpla la condición**: la tarea se ejecutará tras un suceso especificado.

No ejecutar la tarea si está funcionando con batería: la tarea no se iniciará si el ordenador está funcionando con batería en el momento en que está programado el inicio de la tarea. Esto también se aplica a los ordenadores que funcionan con SAI (sistema de alimentación ininterrumpida).

5.10.4 Repetición de la tarea: Diariamente

La tarea se ejecutará todos los días a la hora especificada.

5.10.5 Repetición de la tarea: Semanalmente

La tarea se ejecutará el día y a la hora especificados.

5.10.6 Repetición de la tarea: Desencadenada por un suceso

La tarea se puede desencadenar cuando se produzca cualquiera de los sucesos siguientes:

- **Cada vez que se inicie el ordenador.**
- **La primera vez que se inicie el ordenador en el día**
- **Conexión por módem a Internet/VPN**
- **Se hayan actualizado correctamente las firmas de virus**
- **Se hayan actualizado correctamente los componentes del programa**
- **Registro del usuario**
- **Detección de amenazas**

Cuando se programa una tarea desencadenada por un suceso, se puede especificar el intervalo mínimo entre dos finalizaciones de la tarea. Por ejemplo, si inicia sesión en su ordenador varias veces al día, seleccione 24 horas para realizar la tarea solo en el primer inicio de sesión del día y, después, al día siguiente.

5.10.7 Detalles de la tarea: Ejecutar aplicación

En esta tarea se programa la ejecución de una aplicación externa.

- **Archivo ejecutable**: seleccione un archivo ejecutable en el árbol de directorios y haga clic en la opción **...**, o introduzca la ruta manualmente.
- **Carpeta de trabajo**: defina el directorio de trabajo de la aplicación externa. Todos los archivos temporales del **archivo ejecutable** seleccionado se crearán en este directorio.
- **Parámetros**: parámetros de la línea de comandos de la aplicación (opcional).

Haga clic en **Finalizar** para aplicar la tarea.

5.10.8 Detalles de la tarea - Enviar informes de cuarentena de correo electrónico

Esta tarea programa el envío por correo electrónico de un informe de la Cuarentena de correo electrónico.

- **Dirección del remitente**: especifique la dirección de correo electrónico que se mostrará como remitente del informe de la Cuarentena de correo electrónico.
- **Número máximo de registros en el informe**: puede limitar el número de entradas por informe. El número predeterminado está establecido en 50.
- **URL web**: esta URL se incluirá en el informe de la Cuarentena de correo electrónico, para que el destinatario pueda hacer clic en ella para acceder a la interfaz web de la Cuarentena de correo electrónico.
- **Destinatarios**: seleccione los usuarios que recibirán los informes de la Cuarentena de correo electrónico. Haga clic en **Editar** para seleccionar los buzones de correo para destinatarios concretos. Puede seleccionar varios destinatarios.

Haga clic en **Finalizar** para crear la tarea programada.

5.10.9 Tarea omitida

Si la tarea no se pudo ejecutar en el momento predefinido, puede especificar cuándo se ejecutará:

- **En la siguiente hora programada**: la tarea se ejecutará a la hora especificada (por ejemplo, cuando hayan transcurrido 24 horas).
- **Lo antes posible**: la tarea se ejecutará lo antes posible, cuando las acciones que impidan la ejecución de la tarea ya no sean válidas.
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado**: **Tiempo desde la última ejecución (horas)**: cuando haya seleccionado esta opción, la tarea se repetirá siempre tras el período de tiempo especificado (en horas).

5.10.10 Detalles de la tarea planificada

En este cuadro de diálogo se muestra información detallada sobre la tarea programada seleccionada al hacer doble clic en una tarea personalizada o al hacer clic con el botón derecho del ratón en una tarea personalizada del planificador de tareas y, a continuación, hacer clic en **Mostrar detalles de la tarea**.

5.10.11 Perfiles de actualización

Si desea actualizar el programa desde dos servidores de actualización, es necesario crear dos perfiles de actualización diferentes. Así, si el primer servidor no descarga los archivos de actualización, el programa cambia al otro automáticamente. Esta función es útil para portátiles, por ejemplo, ya que normalmente se actualizan desde un servidor de actualización LAN local, aunque sus propietarios suelen conectarse a Internet utilizando otras redes. Así pues, en caso de que el primer perfil falle, el segundo descargará automáticamente los archivos de actualización de los servidores de actualización de ESET.

Encontrará más información sobre los perfiles de actualización en el capítulo Actualización.

5.10.12 Creación de tareas nuevas

Para crear una tarea nueva en Tareas programadas, haga clic en el botón **Agregar tarea** o haga clic con el botón derecho y seleccione **Agregar** en el menú contextual. Están disponibles cinco tipos de tareas programadas:

- **Ejecutar aplicación externa**: programa la ejecución de una aplicación externa.
- **Mantenimiento de registros**: los archivos de registro también contienen restos de los registros eliminados. Esta tarea optimiza periódicamente los registros incluidos en los archivos para aumentar su eficacia.
- **Verificación de archivos en el inicio del sistema**: comprueba los archivos que se pueden ejecutar al encender o iniciar el sistema.
- **Crear un informe del estado del sistema**: crea una instantánea del ordenador de ESET SysInspector recopila información detallada sobre los componentes del sistema (por ejemplo controladores, aplicaciones) y evalúa el nivel de riesgo de cada componente.
- **Análisis del ordenador**: analiza los archivos y las carpetas del ordenador.
- **Primer análisis**: de forma predeterminada, 20 minutos después de la instalación o el reinicio se realizará un análisis del ordenador como una tarea de prioridad baja.
- **Actualización**: programa una tarea de actualización mediante la actualización de la base de firmas de virus y los módulos del programa.

La **actualización** es una de las tareas programadas más frecuentes, por lo que explicaremos cómo se agrega una nueva tarea de actualización.

Escriba el nombre de la tarea en el campo **Nombre de la tarea**. En el menú desplegable **Tipo de tarea**, seleccione **Actualización** y haga clic en **siguiente**.
Active la opción **Activado** si desea activar la tarea (puede hacerlo más adelante mediante la casilla de verificación situada en la lista de tareas programas), haga clic en **Siguiente** y seleccione una de las opciones de programación: **Una vez**, **Reiteradamente**, **Diariamente**, **Semanalmente** y **Cuando se cumpla la condición**. Según la frecuencia seleccionada, se le solicitarán diferentes parámetros de actualización. A continuación, defina la acción que debe llevarse a cabo si la tarea no se puede realizar o completar a la hora programada. Están disponibles las tres opciones siguientes:

- **En la siguiente hora programada**
- **Lo antes posible**
- **Inmediatamente, si la hora desde la última ejecución excede un valor especificado** (el intervalo se puede definir con el cuadro Tiempo desde la última ejecución)

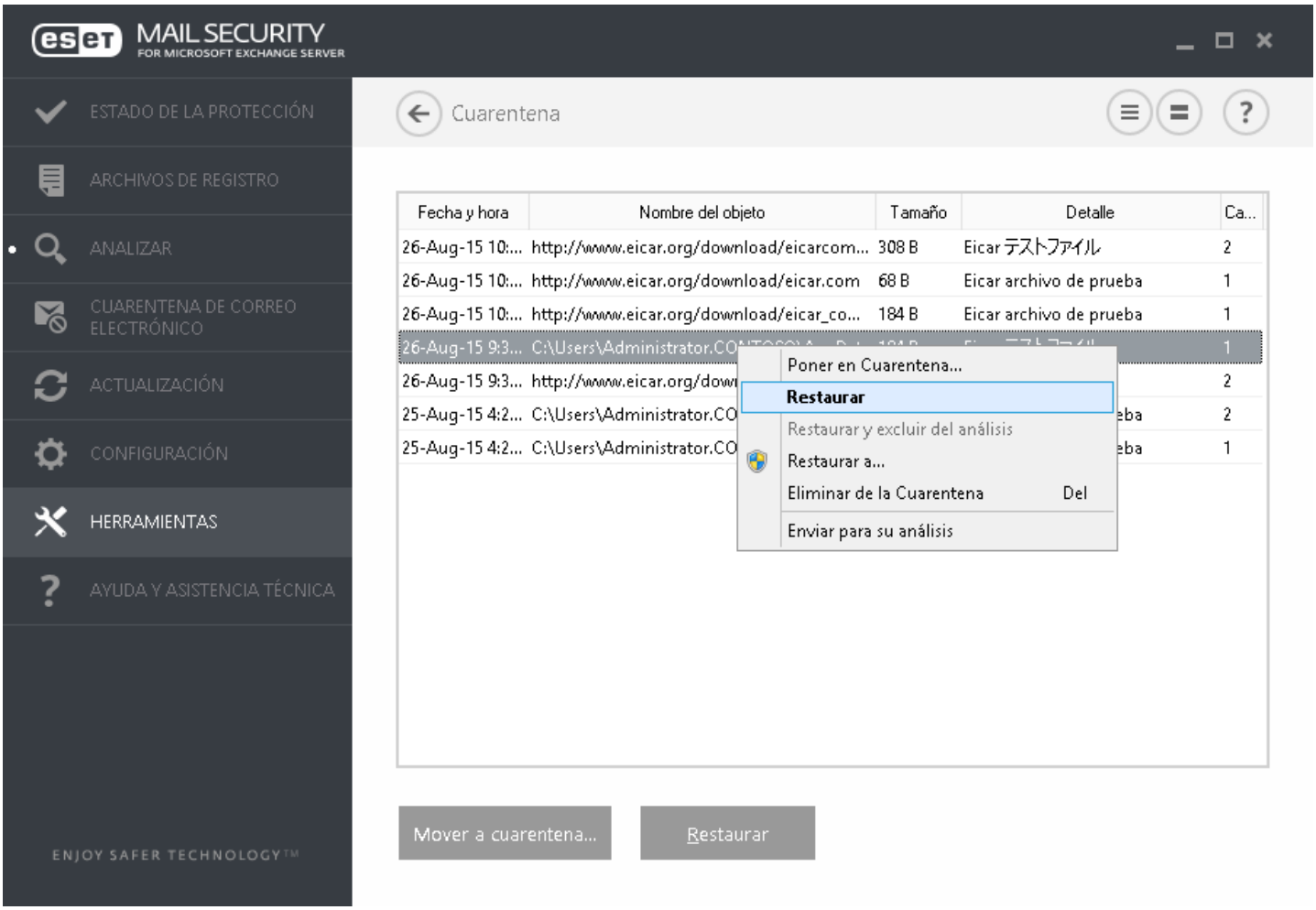
En el paso siguiente se muestra una ventana de resumen que contiene información acerca de la tarea programada actualmente. Haga clic en **Finalizar** cuando haya terminado de hacer cambios.

Aparecerá un cuadro de diálogo que permite al usuario elegir los perfiles que desea utilizar para la tarea programada. Aquí puede definir los perfiles principal y alternativo. El perfil alternativo se utiliza cuando la tarea no se puede completar con el perfil principal. Haga clic en **Finalizar** para confirmar la operación; la nueva tarea se agregará a la lista de tareas programadas.

5.11 Cuarentena

La función principal de la cuarentena es almacenar los archivos infectados de forma segura. Los archivos deben ponerse en cuarentena si no es posible desinfectarlos, si no es seguro ni aconsejable eliminarlos o si ESET Mail Security los detecta incorrectamente como infectados.

Es posible poner en cuarentena cualquier archivo. La cuarentena se recomienda cuando el comportamiento de un archivo es sospechoso y el análisis no lo ha detectado. Los archivos en cuarentena se pueden enviar para su análisis al laboratorio de virus de ESET.



Los archivos almacenados en la carpeta de cuarentena se pueden ver en una tabla que muestra la fecha y la hora en que se pusieron en cuarentena, la ruta de la ubicación original del archivo infectado, su tamaño en bytes, el motivo (agregado por el usuario, por ejemplo) y el número de amenazas (por ejemplo, si se trata de un archivo comprimido que contiene varias amenazas).

En el caso de que los objetos del mensaje de correo electrónico se pongan en cuarentena en la cuarentena de archivos, se mostrará información en forma de ruta al buzón de correo, la carpeta o el nombre del archivo.

Puesta de archivos en cuarentena

ESET Mail Security pone los archivos eliminados en cuarentena automáticamente (si no ha desactivado esta opción en la ventana de alerta). Si lo desea, puede copiar en cuarentena cualquier archivo sospechoso de forma manual, haciendo clic en el botón **Poner en cuarentena.** Los archivos que se pongan en cuarentena se quitarán de su ubicación original. El menú contextual también se puede utilizar con este fin: haga clic con el botón derecho en la ventana **Cuarentena** y seleccione **Poner en cuarentena**.

Restauración de archivos de cuarentena

Los archivos puestos en cuarentena se pueden restaurar a su ubicación original. Para ello, utilice la función **Restaurar**, disponible en el menú contextual que se abre al hacer clic con el botón derecho del ratón en la ventana Cuarentena. Si el archivo está marcado como aplicación potencialmente no deseada, también estará disponible la opción **Restaurar y excluir del análisis**. Puede obtener más información sobre este tipo de aplicación en el glosario. El menú contextual también ofrece la opción **Restaurar a...**, que le permite restaurar archivos en una ubicación distinta a la original de la cual se eliminaron.

NOTA: si el programa ha puesto en cuarentena un archivo no dañino por error, exclúyalo del análisis después de restaurarlo y enviarlo al servicio de atención al cliente de ESET.

Envío de un archivo de cuarentena

Si ha copiado en cuarentena un archivo sospechoso que el programa no ha detectado o si se ha determinado incorrectamente que un archivo está infectado (por ejemplo, por el análisis heurístico del código) y, consecuentemente, se ha copiado a cuarentena, envíe el archivo al laboratorio de virus de ESET. Para enviar un archivo de cuarentena, haga clic con el botón derecho del ratón en el archivo y seleccione **Enviar para su análisis** en el menú contextual.

5.11.1 Copiar archivos en cuarentena

ESET Mail Security pone los archivos eliminados en cuarentena automáticamente (si no ha desactivado esta opción en la ventana de alerta). Si lo desea, puede copiar en cuarentena cualquier archivo sospechoso de forma manual, haciendo clic en el botón **Poner en cuarentena**. En este caso, el archivo original no se elimina de su ubicación original. El menú contextual también se puede utilizar con este fin: haga clic con el botón derecho en la ventana **Cuarentena** y seleccione **Poner en cuarentena**.

5.11.2 Restauración de archivos de cuarentena

Los archivos puestos en cuarentena se pueden restaurar a su ubicación original. Si desea restaurar un archivo puesto en cuarentena, haga clic en él con el botón derecho del ratón en la ventana Cuarentena y seleccione **Restaurar** en el menú contextual. Si el archivo está marcado como aplicación potencialmente no deseada, también estará disponible la opción **Restaurar y excluir del análisis**. El menú contextual también contiene la opción **Restaurar a...**, que le permite restaurar archivos en una ubicación distinta a la original de la cual se eliminaron.

Eliminación de la cuarentena: haga clic con el botón derecho del ratón en el elemento que desee y seleccione **Eliminar de la cuarentena**, o seleccione el elemento que desee eliminar y pulse **Suprimir** en el teclado. Es posible seleccionar varios elementos y eliminarlos al mismo tiempo.

NOTA: si el programa ha puesto en cuarentena un archivo no dañino por error, exclúyalo del análisis después de restaurarlo y enviarlo al servicio de atención al cliente de ESET.

5.11.3 Envío de un archivo a cuarentena

Si ha puesto en cuarentena un archivo sospechoso que el programa no ha detectado o si un archivo se ha evaluado incorrectamente como infectado (por ejemplo, por el análisis heurístico del código) y, consecuentemente, este se ha puesto en cuarentena, envíe el archivo al laboratorio de ESET. Para enviar un archivo de cuarentena, haga clic con el botón derecho del ratón en el archivo y seleccione **Enviar para su análisis** en el menú contextual.

5.12 Actualizaciones del sistema operativo

En la ventana de actualizaciones del sistema se muestra la lista de actualizaciones disponibles que están listas para su descarga e instalación. El nivel de prioridad de la actualización se muestra junto al nombre de la misma.

Haga clic en **Ejecutar actualización del sistema** para iniciar la descarga e instalar las actualizaciones del sistema operativo.

Haga clic con el botón derecho del ratón en cualquier fila de actualización y, a continuación, haga clic en **Mostrar información** para abrir una ventana emergente con información adicional.

6. Glosario

6.1 Tipos de amenazas

Una amenaza es un software malicioso que intenta entrar en el ordenador de un usuario y dañarlo.

6.1.1 Virus

Un virus informático es una amenaza que daña los archivos del ordenador. Su nombre se debe a los virus biológicos, ya que usan técnicas similares para pasar de un ordenador a otro.

Los virus informáticos atacan principalmente a los archivos y documentos ejecutables. Para reproducirse, un virus adjunta su "cuerpo" al final de un archivo de destino. En resumen, así es como funciona un virus informático: después de la ejecución del archivo infectado, el virus se activa (antes de la aplicación original) y realiza la tarea que tiene predefinida. Después, se ejecuta la aplicación original. Un virus no puede infectar un ordenador a menos que un usuario (bien accidental o deliberadamente) ejecute o abra el programa malintencionado.

Los virus informáticos pueden tener diversos fines y niveles de gravedad. Algunos son muy peligrosos, debido a su capacidad para eliminar archivos del disco duro de forma deliberada. Sin embargo, otros virus no causan daños reales, solo sirven para molestar al usuario y demostrar las capacidades técnicas de sus autores.

Es importante mencionar que los virus (si se comparan con los troyanos o el spyware) son cada vez menos habituales, ya que no son atractivos desde un punto de vista comercial para los autores de software malintencionado. Además, el término "virus" se utiliza incorrectamente con mucha frecuencia para abarcar todo tipo de amenazas. Este término está desapareciendo gradualmente y se está sustituyendo por el término "malware" (software malicioso), que es más preciso.

Si su ordenador se infecta con un virus, debe restaurar los archivos infectados a su estado original, es decir, desinfectarlos con un programa antivirus.

Ejemplos de virus:: OneHalf, Tenga y Yankee Doodle.

6.1.2 Gusanos

Un gusano informático es un programa que contiene código malicioso que ataca a los ordenadores host y se extiende a través de una red. La principal diferencia entre un virus y un gusano es que los gusanos tienen la capacidad de reproducirse y viajar solos, no dependen de archivos host (o sectores de inicio). Los gusanos se extienden por las direcciones de correo electrónico de la lista de contactos o explotan las vulnerabilidades de seguridad de las aplicaciones de red.

Los gusanos son mucho más viables que los virus informáticos; dada la gran disponibilidad de Internet, se pueden extender por todo el mundo en cuestión de horas, o incluso minutos, desde su lanzamiento. Esta capacidad para reproducirse de forma independiente y rápida los hace más peligrosos que otros tipos de código malicioso.

Un gusano activado en un sistema puede causar una serie de problemas: puede eliminar archivos, degradar el rendimiento del sistema o incluso desactivar algunos programas. Además, su naturaleza le permite servir de "medio de transporte" para otros tipos de amenazas.

Si el ordenador está infectado con un gusano, es recomendable eliminar los archivos infectados, pues podrían contener código malicioso.

Ejemplos de gusanos conocidos: Lovsan/Blaster, Stration/Warezov, Bagle y Netsky.

6.1.3 Caballos troyanos

Históricamente, los troyanos informáticos se han definido como una clase de amenaza que intenta presentarse como un programa útil, engañando así a los usuarios para que permitan su ejecución. Sin embargo, es importante señalar que esto era así en el caso de los caballos troyanos del pasado; hoy en día, ya no necesitan disfrazarse. Su único fin es infiltrarse lo más fácilmente posible y cumplir sus malintencionados objetivos. "Troyano" se ha convertido en un término muy general para describir cualquier amenaza que no entre en ninguna clase de amenaza específica.

Dado que se trata de una categoría muy amplia, con frecuencia se divide en muchas subcategorías:

- **Programas de descarga**: programa malintencionado con capacidad para descargar otras amenazas de Internet.
- **Lanzador**: tipo de troyano diseñado para lanzar otros tipos de código malicioso en ordenadores vulnerables.
- **Puerta trasera**: aplicación que se comunica con atacantes remotos y les permite acceder a los sistemas para tomar su control.
- **Registrador de pulsaciones**: programa que registra todas las teclas pulsadas por el usuario y envía la información a atacantes remotos.
- **Marcador**: los marcadores son programas diseñados para conectar con números de tarifa con recargo. Es casi imposible que un usuario note que se ha creado una conexión. Los marcadores solo pueden causar daño a los usuarios con módems de marcación, que ya casi no se utilizan.

Normalmente, los troyanos adoptan la forma de archivos ejecutables con la extensión .exe. Si se detecta un archivo como troyano en su ordenador, es recomendable que lo elimine, ya que lo más probable es que contenga código malicioso.

Ejemplos de troyanos conocidos:: NetBus, Trojandownloader. Small.ZL, Slapper.

6.1.4 Rootkits

Los rootkits son programas malintencionados que conceden a los atacantes de Internet acceso ilimitado a un sistema, al tiempo que ocultan su presencia. Una vez que han accedido al sistema (normalmente aprovechando alguna vulnerabilidad del mismo), usan funciones del sistema operativo para evitar su detección por parte del antivirus: ocultan procesos, archivos y datos de registro de Windows, etc. Por este motivo, es casi imposible detectarlos con las técnicas de detección normales.

Hay dos niveles de detección disponibles para evitar los rootkits:

1) Cuando intentan acceder a un sistema. Aún no están presentes y, por tanto, están inactivos. La mayoría de los sistemas antivirus pueden eliminar rootkits en este nivel (suponiendo que realmente detectan dichos archivos como infectados).
2) Cuando se ocultan en el proceso normal de análisis. Los usuarios de ESET Mail Security tienen la ventaja de la tecnología Anti-Stealth, que también puede detectar y eliminar rootkits activos.

6.1.5 Adware

Adware es la abreviatura del término inglés utilizado para el software relacionado con publicidad. Los programas que muestran material publicitario se incluyen en esta categoría. Normalmente, las aplicaciones de adware abren automáticamente una ventana emergente nueva con anuncios en el navegador de Internet o cambian la página de inicio del navegador. La aplicación de adware suele instalarse con programas gratuitos, lo que permite a los creadores de esos programas gratuitos cubrir los costes de desarrollo de sus aplicaciones (normalmente útiles).

La aplicación de adware no es peligrosa en sí, pero molesta a los usuarios con publicidad. El peligro reside en el hecho de que la aplicación de adware también puede realizar funciones de seguimiento (al igual que las aplicaciones de spyware).

Si decide utilizar un producto gratuito, preste especial atención al programa de instalación. La mayoría de los instaladores le informarán sobre la instalación de un programa de adware adicional. Normalmente, podrá cancelarlo

e instalar el programa sin esta aplicación de adware.

Sin embargo, algunos programas no se instalarán sin la aplicación de adware, o su funcionalidad será limitada. Esto significa que la aplicación de adware puede acceder al sistema de manera "legal" a menudo, pues los usuarios así lo han aceptado. En este caso, es mejor adoptar un enfoque seguro que tener que lamentarse. Si se detecta un archivo de adware en su ordenador, es aconsejable que lo elimine, ya que es muy posible que contenga código malicioso.

6.1.6 Spyware

Esta categoría abarca todas las aplicaciones que envían información privada sin el consentimiento o conocimiento del usuario. El spyware usa funciones de seguimiento para enviar diversos datos estadísticos, como una lista de sitios web visitados, direcciones de correo electrónico de la lista de contactos del usuario o una lista de palabras escritas.

Los autores de spyware afirman que el objetivo de estas técnicas es averiguar más sobre las necesidades y los intereses de los usuarios, así como permitir una publicidad mejor gestionada. El problema es que no existe una distinción clara entre las aplicaciones útiles y las malintencionadas, de modo que nadie puede estar seguro de que no se hará un mal uso de la información recuperada. Los datos obtenidos por aplicaciones spyware pueden contener códigos de seguridad, códigos PIN, números de cuentas bancarias, etc. Con frecuencia, el spyware se envía junto con versiones gratuitas de programas para generar ingresos u ofrecer un incentivo para comprar el software. A menudo, se informa a los usuarios sobre la presencia de spyware durante la instalación de un programa para ofrecerles un incentivo para la adquisición de una versión de pago.

Algunos ejemplos de productos gratuitos conocidos que se envían junto con spyware son las aplicaciones cliente de redes P2P (punto a punto). Spyfalcon o Spy Sheriff (y muchos más) pertenecen a una subcategoría específica de spyware: parecen programas antispyware, pero en realidad son aplicaciones de spyware.

Si se detecta un archivo de spyware en su ordenador, es aconsejable que lo elimine, ya que es muy posible que contenga código malicioso.

6.1.7 Empaquetadores

Un empaquetador es un archivo ejecutable autoextraíble en tiempo de ejecución que combina varios tipos de código malicioso en un solo paquete.

Los más comunes son UPX, PE_Compact, PKLite y ASPack. El mismo código malicioso se puede detectar de forma diferente cuando se comprime con un empaquetador diferente. Los empaquetadores también tienen la capacidad de hacer que sus "firmas" muten con el tiempo, haciendo que el código malicioso sea más difícil de detectar y eliminar.

6.1.8 Bloqueador de exploits

El Bloqueador de exploits se ha diseñado para fortificar aquellas aplicaciones que sufren más ataques, como los navegadores de Internet, los lectores de archivos PDF, los clientes de correo electrónico y los componentes de MS Office. Este producto supervisa el comportamiento de los procesos en busca de actividad sospechosa que pueda indicar la presencia de un exploit. Además añade otra capa de protección, un paso más cerca de los atacantes, con una tecnología totalmente diferente en comparación con las técnicas centradas en la detección de archivos maliciosos.

Cuando detecta un proceso sospechoso, el Bloqueador de exploits lo detiene inmediatamente y registra los datos de la amenaza; después los envía al sistema de nube de ESET Live Grid. El laboratorio de amenazas de ESET procesa estos datos y los utiliza para mejorar la protección que ofrece a los usuarios frente a amenazas desconocidas y ataques 0-day (código malicioso reciente para que el que no hay ninguna solución preconfigurada).

6.1.9 Análisis avanzado de memoria

El Análisis avanzado de memoria trabaja conjuntamente con el Bloqueador de exploits para mejorar la protección frente a código malicioso, que utiliza los métodos de ofuscación y cifrado para evitar su detección mediante productos de protección frente a este tipo de código. En aquellos casos en los que la emulación o la heurística normales no detectan una amenaza, el Análisis de memoria avanzado consigue identificar comportamientos sospechosos y analiza las amenazas que se presentan en la memoria del sistema. Esta solución es eficaz incluso para código malicioso muy ofuscado. A diferencia del Bloqueador de exploits, se trata de un método posterior a la ejecución, lo cual significa que existe la posibilidad de que haya habido actividad maliciosa antes de la detección de una amenaza. No obstante, ofrece una capa de seguridad adicional cuando las otras técnicas de detección fallan.

6.1.10 Aplicaciones potencialmente peligrosas

Existen muchos programas legítimos que sirven para simplificar la administración de ordenadores en red. Sin embargo, si caen en las manos equivocadas, pueden utilizarse con fines maliciosos. ESET Mail Security proporciona una opción para detectar estas amenazas.

Aplicaciones potencialmente peligrosas es la clasificación utilizada para el software comercial legítimo. Esta clasificación incluye programas como herramientas de acceso remoto, aplicaciones para detectar contraseñas y registradores de pulsaciones (programas que graban todas las teclas pulsadas por un usuario).

Si detecta la presencia de una aplicación potencialmente peligrosa que esté en ejecución en su ordenador (y no la ha instalado usted), consulte con el administrador de la red o elimine la aplicación.

6.1.11 Aplicaciones potencialmente indeseables

Las **aplicaciones potencialmente indeseables** (PUA) no tienen por qué ser maliciosas, pero pueden afectar negativamente al rendimiento del ordenador. Dichas aplicaciones suelen necesitar el consentimiento del usuario para su instalación. Si se encuentran en su ordenador, el sistema se comportará de manera diferente (en comparación con el estado en el que se encontraba antes de la instalación). Los cambios más importantes son:

- Se abren ventanas nuevas que no se habían visto anteriormente (como ventanas emergentes y anuncios).
- Activación y ejecución de procesos ocultos.
- Mayor uso de los recursos del sistema.
- Cambios en los resultados de búsqueda.
- La aplicación se comunica con servidores remotos.

6.2 Correo electrónico

El correo electrónico es una forma de comunicación moderna que ofrece muchas ventajas: es flexible, rápido y directo; y tuvo un papel fundamental en la expansión de Internet a principios de los años 90.

Lamentablemente, a causa de su alto nivel de anonimato, el correo electrónico e Internet dan cabida a actividades ilegales como la distribución de correo no deseado. El correo no deseado incluye anuncios no solicitados, información falsa y la difusión de software malicioso (código malicioso). Sus inconvenientes y peligros para el usuario son mayores porque el envío de correo no deseado tiene un coste mínimo, y los autores de este tipo de correo disponen de muchas herramientas para obtener nuevas direcciones de correo electrónico. Además, la cantidad y la variedad de correo no deseado dificulta en gran medida su regulación. Cuanto más utilice su dirección de correo electrónico, mayores serán las posibilidades de que acabe en la base de datos de un motor de correo no deseado. A continuación, le ofrecemos algunos consejos para su prevención:

- Si es posible, no publique su dirección de correo electrónico en Internet.
- Proporcione su dirección de correo electrónico únicamente a personas de confianza.
- Si es posible, no utilice alias muy comunes; cuanto más complicados sean, menor será la posibilidad de que puedan obtenerlos.
- No conteste a mensajes de correo no deseado que hayan llegado a su buzón de correo.

- Tenga cuidado cuando rellene formularios en Internet, preste especial atención a casillas como "Sí, deseo recibir información".
- Utilice direcciones de correo electrónico "especializadas"; por ejemplo, una para el trabajo, otra para comunicarse con sus amigos, etc.
- Cambie su dirección de correo electrónico periódicamente.
- Utilice una solución antispam.

6.2.1 Publicidad

La publicidad en Internet es una de las formas de publicidad que presentan un crecimiento más rápido. Sus principales ventajas de marketing son los costes mínimos, un contacto muy directo y, lo más importante, el hecho de que los mensajes se entregan de forma casi inmediata. Muchas empresas utilizan herramientas de marketing por correo electrónico para comunicarse eficazmente con sus clientes actuales y potenciales.

Este tipo de publicidad es legítimo, ya que es posible que el usuario esté interesado en recibir información comercial sobre algunos productos. No obstante, son muchas las empresas que envían mensajes publicitarios no deseados en serie. En estos casos, la publicidad por correo electrónico cruza la línea y se convierte en correo no deseado.

Actualmente, la enorme cantidad de correo no solicitado constituye un problema y no tiene visos de disminuir. Los autores de correos electrónicos no solicitados intentan disfrazar el correo no deseado como mensajes legítimos.

6.2.2 Información falsa

La información falsa se extiende a través de Internet. Normalmente, la información falsa se envía mediante herramientas de comunicación o correo electrónico como ICQ y Skype. El mensaje en sí suele ser una broma o una leyenda urbana.

La información falsa sobre virus de ordenador pretende generar miedo, incertidumbre y duda en los destinatarios, haciéndoles creer que existe un "virus indetectable" que elimina archivos y recupera contraseñas, o que realiza ciertas acciones que pueden provocar daños en el sistema.

Algunos elementos de información falsa solicitan a los destinatarios que reenvíen los mensajes a sus contactos, divulgando así dicha información. La información falsa también se transmite a través de teléfonos móviles, peticiones de ayuda, personas que se ofrecen a enviarle dinero desde países extranjeros, etc. Por lo general, es imposible averiguar la intención del creador.

Si recibe un mensaje donde se le solicita que lo reenvíe a todas las personas que conozca, es muy probable que se trate de información falsa. En Internet encontrará muchos sitios web que pueden verificar la legitimidad de un mensaje de correo electrónico. Antes de reenviarlo, realice una búsqueda en Internet sobre cualquier mensaje que sospeche que contiene información falsa.

6.2.3 Phishing

El término phishing define una actividad delictiva que usa técnicas de ingeniería social (manipulación de los usuarios para obtener información confidencial). Su objetivo es acceder a datos confidenciales como números de cuentas bancarias, códigos PIN, etc.

Normalmente, el acceso se consigue enviando correos electrónicos con remitentes disfrazados de personas o empresas serias (instituciones financieras, compañías de seguros, etc.). La apariencia del correo electrónico puede ser real, y contener gráficos y texto originales de la fuente por la que desean hacerse pasar. En el mensaje se le pide que escriba, con varios pretextos (verificación de datos, operaciones financieras), algunos de sus datos personales: números de cuentas bancarias o nombres de usuario y contraseñas. Dichos datos, si se envían, pueden ser fácilmente sustraídos o utilizados de forma fraudulenta.

Los bancos, las compañías de seguros y otras empresas legítimas nunca le pedirán sus nombres de usuario y contraseña en un correo electrónico no solicitado.

6.2.4 Reconocimiento de correo no deseado no solicitado

Por lo general, existen varios indicadores que pueden ayudarle a identificar el correo no deseado (spam) en su buzón de correo. Si un mensaje cumple, como mínimo, una de las siguientes condiciones, es muy probable que se trate de un mensaje de correo no deseado:

- La dirección del remitente no pertenece a ninguna persona de su lista de contactos.
- El mensaje le ofrece una gran cantidad de dinero, pero tiene que proporcionar una pequeña cantidad previamente.
- El mensaje le solicita que introduzca, con varios pretextos (verificación de datos, operaciones financieras), algunos de sus datos personales (números de cuentas bancarias, nombres de usuario y contraseñas, etc.).
- Está escrito en otro idioma.
- Le solicita que adquiera un producto en el que no está interesado. Si decide comprarlo de todos modos, compruebe que el remitente del mensaje corresponde a un identificador fiable (consulte al fabricante del producto original).
- Algunas palabras están mal escritas para intentar engañar a su filtro de correo no deseado. Por ejemplo, "vaigra" en lugar de "viagra", entre otros.

6.2.4.1 Reglas

En el contexto de las soluciones antispam y los clientes de correo electrónico, las reglas son herramientas para manipular funciones de correo electrónico que constan de dos partes lógicas:

1) Condición (por ejemplo, un mensaje entrante de una dirección concreta).

2) Acción (por ejemplo, la eliminación del mensaje o su transferencia a una carpeta específica).

El número y la combinación de reglas varía en función de la solución antispam. Estas reglas sirven como medidas contra el correo no deseado. Ejemplos típicos:

- Condición: un correo electrónico entrante contiene algunas palabras que suelen aparecer en los mensajes de correo no deseado 2. Acción: eliminar el mensaje.
- Condición: un correo electrónico entrante contiene un archivo adjunto con una extensión .exe 2. Acción: eliminar el archivo adjunto y enviar el mensaje al buzón de correo.
- Condición: recibe un correo electrónico entrante de su jefe 2. Acción: mover el mensaje a la carpeta "Trabajo".

Es recomendable que, en los programas antispam, use una combinación de reglas para facilitar la administración y filtrar el correo no deseado de forma más eficaz.

6.2.4.2 Filtro Bayesiano

El filtro Bayesiano de correo no deseado es una forma efectiva de filtrar correo electrónico que utilizan casi todos los productos antispam. Este filtro identifica el correo no solicitado con una gran precisión y funciona de forma individual para cada usuario.

La funcionalidad se basa en el principio siguiente: el proceso de aprendizaje tiene lugar en la primera fase. El usuario marca manualmente un número suficiente de mensajes como mensajes legítimos o como correo no deseado (normalmente 200/200). El filtro analiza ambas categorías y aprende, por ejemplo, que el correo no deseado contiene las palabras "rolex" o "viagra" y que los mensajes legítimos proceden de familiares o de direcciones incluidas en la lista de contactos del usuario. Si se procesa un número adecuado de mensajes, el filtro Bayesiano puede asignar un "índice de correo no deseado" a cada mensaje para determinar si es spam o no.

La principal ventaja del filtro Bayesiano es su flexibilidad. Por ejemplo, si un usuario es biólogo, normalmente todos los correos electrónicos entrantes sobre biología o campos de estudio relacionados recibirán un índice de probabilidad inferior. Si un mensaje incluye palabras que normalmente lo clasificarían como no solicitado, pero lo envía alguien de la lista de contactos del usuario, este se marcará como legítimo, ya que los remitentes de una lista

de contactos reducen la probabilidad general de correo no deseado.

6.2.4.3 Lista blanca

Por lo general, una lista blanca es una lista de elementos o personas aceptados o a los que se ha concedido permiso. El término "lista blanca de correo electrónico" es una lista de contactos de los que el usuario desea recibir mensajes. Estas listas blancas se basan en palabras clave que se buscan en direcciones de correo electrónico, nombres de dominios o direcciones IP.

Si una lista blanca funciona en "modo de exclusividad", no se recibirán los mensajes procedentes de otras direcciones, dominios o direcciones IP. Si la lista no es exclusiva, estos mensajes no se eliminarán, sino que se filtrarán de alguna otra forma.

Las listas blancas se basan en el principio opuesto al de las listas negras. Las listas blancas son relativamente fáciles de mantener, más que las listas negras. Es recomendable que use tanto una lista blanca como una lista negra para filtrar el correo no deseado de forma más eficaz.

6.2.4.4 Lista negra

Por lo general, una lista negra es una lista de personas o elementos prohibidos o no aceptados. En el mundo virtual, es una técnica que permite aceptar mensajes de todos los usuarios que no se incluyan en dicha lista.

Existen dos tipos de listas negras: las que crean los usuarios con su aplicación antispam y las profesionales, creadas por instituciones especializadas que las actualizan periódicamente y que se pueden encontrar en Internet.

Las listas negras son esenciales para bloquear con éxito el correo no deseado; sin embargo, son difíciles de mantener, ya que todos los días aparecen nuevos elementos que se deben bloquear. Le recomendamos que utilice una lista blanca y una lista negra para filtrar con mayor eficacia el correo no deseado.

6.2.4.5 Control del servidor

El control del servidor es una técnica que sirve para identificar correo electrónico no deseado en masa a partir del número de mensajes recibidos y las reacciones de los usuarios. Cada mensaje deja una "huella" digital única basada en el contenido del mensaje. El número de identificación exclusivo no indica nada sobre el contenido del mensaje de correo electrónico. Dos mensajes idénticos tendrán huellas idénticas, mientras que los mensajes diferentes tendrán huellas diferentes.

Si se marca un mensaje como no deseado, su huella se envía al servidor. Si el servidor recibe más huellas idénticas (correspondientes a un determinado mensaje no deseado), la huella se guarda en la base de datos de huellas de correo no deseado. Al analizar mensajes entrantes, el programa envía las huellas de los mensajes al servidor que, a su vez, devuelve información sobre las huellas correspondientes a los mensajes ya marcados por los usuarios como no deseados.